Garg, Yogesh

From: Patel, Jagdish N.
Sent: Monday, February 13, 2006 6:43 PM
To: Garg, Yogesh
Subject: search 09/906,995 date: 2/13/2006

```
Trying 31060000009999...Open

DIALOG INFORMATION SERVICES
PLEASE LOGON:
******** HHHHHHHH SSSSSSSS? ### Status: Signing onto Dialog ********
ENTER PASSWORD:
******** HHHHHHHH SSSSSSSS? ********
### Status: Login successfulWelcome to DIALOG

Dialog level 05.10.03D

Last logoff: 12feb06 12:19:12
Logon file405 13feb06 18:18:51
*** ANNOUNCEMENT ***
***
NEW FILES RELEASED
***Index Chemicus (File 302)
***Inspec (File 202)
***Physical Education Index (File 138)
***
RELOADS COMPLETED
*** The 2005 reload of the CLAIMS files (Files 340, 341, 942)
is now available online.

RESUMED UPDATING
***ERIC (File 1)
***
Chemical Structure Searching now available in Prous Science Drug
Data Report (F452), Prous Science Drugs of the Future (F453),
IMS R&D Focus (F445/955), Pharmaprojects (F128/928), Beilstein
Facts (F390), Derwent Chemistry Resource (F355) and Index Chemicus
(File 302).
***
>>> Enter BEGIN HOMEBASE for Dialog Announcements <<<
>>> of new databases, price changes, etc. <<<
****
FTXTCOR is set ON as an alias for 15, 9, 810, 275, 476, 610, 275, 476, 624,
636, 621, 613, 813, 16, 160, 634, 148, 20
NFTXTCOR is set ON as an alias for 77, 35, 583, 65, 2, 233, 474, 475, 99,
348,349,347
* * *
SYSTEM:HOME
Cost is in DialUnits
Menu System II: D2 version 1.7.9 term=ASCII
*** DIALOG HOMEBASE(SM) Main Menu ***

Information:
1. Announcements (new files, reloads, etc.)
2. Database, Rates, & Command Descriptions
3. Help in Choosing Databases for Your Topic
```

4. Customer Services (telephone assistance, training, seminars, etc.)
5. Product Descriptions

Connections:
6. DIALOG(R) Document Delivery
7. Data Star(R)

/H = Help /L = Logoff /NOMENU = Command Mode

Enter an option number to view information or to connect to an online service. Enter a BEGIN command plus a file number to search a database (e.g., B1 for ERIC).
?
Terminal set to DLINK
*** DIALOG HOMEBASE(SM) Main Menu ***

Information:
1. Announcements (new files, reloads, etc.)
2. Database, Rates, & Command Descriptions
3. Help in Choosing Databases for Your Topic
4. Customer Services (telephone assistance, training, seminars, etc.)
5. Product Descriptions

Connections:
6. DIALOG(R) Document Delivery
7. Data Star(R)

/H = Help /L = Logoff /NOMENU = Command Mode

Enter an option number to view information or to connect to an online service. Enter a BEGIN command plus a file number to search a database (e.g., B1 for ERIC).
? b ftxtcor nftxtcor

>>> 77 does not exist
>>> 233 does not exist
>>>2 of the specified files are not available
13feb06 18:19:04 User242899 Session D489.1
$0.00 0.213 DialUnits FileHomeBase
$0.00 Estimated cost FileHomeBase
$0.05 TELNET
$0.05 Estimated cost this search
$0.05 Estimated total session cost 0.213 DialUnits

SYSTEM:OS - DIALOG OneSearch
File 15:ABI/Inform(R) 1971-2006/Feb 13
(c) 2006 ProQuest Info&Learning
File 9:Business & Industry(R) Jul/1994-2006/Feb 10
(c) 2006 The Gale Group
File 810:Business Wire 1986-1999/Feb 28
(c) 1999 Business Wire
File 275:Gale Group Computer DB(TM) 1983-2006/Feb 10
(c) 2006 The Gale Group

File 476:Financial Times Fulltext 1982-2006/Feb 14
(c) 2006 Financial Times Ltd
File 610:Business Wire 1999-2006/Feb 13
(c) 2006 Business Wire.
***File 610: File 610 now contains data from 3/99 forward.**
Archive data (1986-2/99) is available in File 810.
File 624:McGraw-Hill Publications 1985-2006/Feb 13
(c) 2006 McGraw-Hill Co. Inc
***File 624: Homeland Security & Defense and 9 Platt energy journals added**
Please see HELP NEWS624 for more
File 636:Gale Group Newsletter DB(TM) 1987-2006/Feb 10
(c) 2006 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2006/Feb 13
(c) 2006 The Gale Group
File 613:PR Newswire 1999-2006/Feb 09
(c) 2006 PR Newswire Association Inc
***File 613: File 613 now contains data from 5/99 forward.**
Archive data (1987-4/99) is available in File 813.
File 813:PR Newswire 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc
File 16:Gale Group PROMT(R) 1990-2006/Feb 10
(c) 2006 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
(c) 1999 The Gale Group
File 634:San Jose Mercury Jun 1985-2006/Feb 11
(c) 2006 San Jose Mercury News
File 148:Gale Group Trade & Industry DB 1976-2006/Feb 13
(c)2006 The Gale Group
File 20:Dialog Global Reporter 1997-2006/Feb 09
(c) 2006 Dialog
File 35:Dissertation Abs Online 1861-2006/Jan
(c) 2006 ProQuest Info&Learning
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
(c) 2002 The Gale Group
***File 583: This file is no longer updating as of 12-13-2002.**
File 65:Inside Conferences 1993-2006/Feb W2
(c) 2006 BLDSC all rts. reserv.
File 2:INSPEC 1898-2006/Jan W4
(c) 2006 Institution of Electrical Engineers
***File 2: Archive data back to 1898 has been added to File 2.**
File 474:New York Times Abs 1969-2006/Feb 12
(c) 2006 The New York Times
File 475:Wall Street Journal Abs 1973-2006/Feb 10
(c) 2006 The New York Times
File 99:Wilson Appl. Sci & Tech Abs 1983-2006/Jan
(c) 2006 The HW Wilson Co.
File 348:EUROPEAN PATENTS 1978-2006/Jan W05
(c) 2006 European Patent Office
***File 348: For important information about IPCR/8 and forthcoming**
changes to the IC= index, see HELP NEWSIPCR.
File 349:PCT FULLTEXT 1979-2006/UB=20060126,UT=20060119
(c) 2006 WIPO/Univentio
***File 349: For important information about IPCR/8 and forthcoming**
changes to the IC= index, see HELP NEWSIPCR.
File 347:JAPIO Nov 1976-2005/Oct(Updated 060203)
(c) 2006 JPO & JAPIO

Set Items Description
--- ----- -----------
? s (frequent adj5 flier)(s) (credit?) (10n) (organization or corporation or

```
company)
0 FREQUENT ADJ5 FLIER
6131238 CREDIT?
4344376 ORGANIZATION
7698245 CORPORATION
42701334 COMPANY
S1 0 (FREQUENT ADJ5 FLIER)(S) (CREDIT?) (10N) (ORGANIZATION OR
CORPORATION OR COMPANY)
? s (FREQUENT ADJ5 FLyer )(S) (CREDIT?) (10N) (ORGANIZATION OR
>>>Possible typing error near end of command
? CORPORATION OR COMPANY)
>>>Operator in invalid position: OR
?
? ds

Set Items Description
S1 0 (FREQUENT ADJ5 FLIER)(S) (CREDIT?) (10N) (ORGANIZATION OR -
CORPORATION OR COMPANY)
? show files
File 15:ABI/Inform(R) 1971-2006/Feb 13
(c) 2006 ProQuest Info&Learning
File 9:Business & Industry(R) Jul/1994-2006/Feb 10
(c) 2006 The Gale Group
File 810:Business Wire 1986-1999/Feb 28
(c) 1999 Business Wire
File 275:Gale Group Computer DB(TM) 1983-2006/Feb 10
(c) 2006 The Gale Group
File 476:Financial Times Fulltext 1982-2006/Feb 14
(c) 2006 Financial Times Ltd
File 610:Business Wire 1999-2006/Feb 13
(c) 2006 Business Wire.
File 624:McGraw-Hill Publications 1985-2006/Feb 13
(c) 2006 McGraw-Hill Co. Inc
File 636:Gale Group Newsletter DB(TM) 1987-2006/Feb 10
(c) 2006 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2006/Feb 13
(c) 2006 The Gale Group
File 613:PR Newswire 1999-2006/Feb 09
(c) 2006 PR Newswire Association Inc
File 813:PR Newswire 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc
File 16:Gale Group PROMT(R) 1990-2006/Feb 10
(c) 2006 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
(c) 1999 The Gale Group
File 634:San Jose Mercury Jun 1985-2006/Feb 11
(c) 2006 San Jose Mercury News
File 148:Gale Group Trade & Industry DB 1976-2006/Feb 13
(c)2006 The Gale Group
File 20:Dialog Global Reporter 1997-2006/Feb 09
(c) 2006 Dialog
File 35:Dissertation Abs Online 1861-2006/Jan
(c) 2006 ProQuest Info&Learning
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
(c) 2002 The Gale Group
File 65:Inside Conferences 1993-2006/Feb W2
(c) 2006 BLDSC all rts. reserv.
File 2:INSPEC 1898-2006/Jan W4
(c) 2006 Institution of Electrical Engineers
File 474:New York Times Abs 1969-2006/Feb 12
```

```
(c) 2006 The New York Times
File 475:Wall Street Journal Abs 1973-2006/Feb 10
(c) 2006 The New York Times
File 99:Wilson Appl. Sci & Tech Abs 1983-2006/Jan
(c) 2006 The HW Wilson Co.
File 348:EUROPEAN PATENTS 1978-2006/Jan W05
(c) 2006 European Patent Office
File 349:PCT FULLTEXT 1979-2006/UB=20060126,UT=20060119
(c) 2006 WIPO/Univentio
File 347:JAPIO Nov 1976-2005/Oct(Updated 060203)
(c) 2006 JPO & JAPIO
? ds

Set Items Description
S1 0 (FREQUENT ADJ5 FLIER)(S) (CREDIT?) (10N) (ORGANIZATION OR -
CORPORATION OR COMPANY)
? s FREQUENT ADJ5 FLyer)(S) (CREDIT?) (10N) (ORGANIZATION OR -
>>>Unmatched parentheses
? CORPORATION OR COMPANY)
>>>Operator in invalid position: OR
?
? s (FREQUENT ADJ5 FLIER)(S) (CREDIT?) (10N) (ORGANIZATION OR -
>>>Unmatched parentheses
? CORPORATION OR COMPANY)
>>>Operator in invalid position: OR
?
? s ((FREQUENT ADJ5 FLIER)(S) (CREDIT?) (10N) (ORGANIZATION OR -
>>>Unmatched parentheses
? CORPORATION OR COMPANY)
>>>Operator in invalid position: OR
?
? s (FREQUENT ADJ5 FLyer)(S) (CREDIT?) (10N) (ORGANIZATION OR -
>>>Unmatched parentheses
? CORPORATION OR COMPANY)
>>>Operator in invalid position: OR
?
? s (FREQUENT (5n) FLyer)(S) (CREDIT?) (10N) (ORGANIZATION OR corporation or
company)
Processing
Processed 10 of 26 files ...
Processing
Processing
Processing
Processing
Processed 20 of 26 files ...
Completed processing all files
707025 FREQUENT
118902 FLYER
6131238 CREDIT?
4344376 ORGANIZATION
7698245 CORPORATION
42701334 COMPANY
S2 786 (FREQUENT (5N) FLYER)(S) (CREDIT?) (10N) (ORGANIZATION OR
CORPORATION OR COMPANY)
? s s2 (s) (data (1w)base) or database)(5n) (employee)

>>>Unmatched parentheses
? s s2 (s) ((data (1w)base) or database)(5n) (employee)
Processing
Processed 10 of 26 files ...
```

Processing
Processed 20 of 26 files ...
Completed processing all files
786 S2
16353461 DATA
6319441 BASE
245816 DATA(1W)BASE
2531221 DATABASE
2095157 EMPLOYEE
S3 0 S2 (S) ((DATA (1W)BASE) OR DATABASE)(5N) (EMPLOYEE)
?
? s s2 (s) (accumulat?) (10n) (mileage or miles)
786 S2
1239673 ACCUMULAT?
122191 MILEAGE
1614524 MILES
S4 16 S2 (S) (ACCUMULAT?) (10N) (MILEAGE OR MILES)
? s s4 and py<2001
Processing
Processed 10 of 26 files ...
Processing
Processed 20 of 26 files ...
Processing
Completed processing all files
16 S4
73938709 PY<2001
S5 11 S4 AND PY<2001
? t s5/9,k/1-11

5/9,K/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01815988 04-66979
"Don't you already have this information?"
Tehrani, Rich
Call Center Solutions v17n3 PP: 12-16 Sep 1998 ISSN: 1521-0774
JRNL CODE: TLM
DOC TYPE: Journal article LANGUAGE: English LENGTH: 3 Pages
WORD COUNT: 1842
GEOGRAPHIC NAMES: US

DESCRIPTORS: Call centers; Customer services; Problems; Credit cards; Airlines
CLASSIFICATION CODES: 2400 (CN=Public relations); 8350 (CN=Transportation industry); 8120 (CN=Retail banking); 9190 (CN=United States)

ABSTRACT: For a company to remain competitive, it needs to have incredible customer service. Two examples of unfortunate encounters with customer service departments, one a credit card company and the other an airline, are presented. Based on these experiences, people are still in the nascent stages of a wonderful technology revolution in the call center.

TEXT: You don't need extensive market research to realize that the call center market is still in its infancy - All you need is a telephone, a mortgage or a credit card.

America's economy is destined to become a service economy. How many times have we heard this? Service companies are making a killing on Wall Street with huge market capitalization numbers and future business projections are

equally impressive.

But for a company to remain competitive, this is only part of the picture Every company needs to have incredible customer service. Insurance, banking, manufacturing...everyone. So as we approach the next millennium, we have made great strides in customer service and the future looks bright. Right? Wrong!

I recently had two encounters, one with a bank and the other with a credit card company, that were absolutely infuriating. I am not in the banking or credit card business, but I can guarantee you that service is the key to long-term growth in both these industries. Bank advertising seems to be at an all-time high: the airwaves are full of radio and television ads, newspapers are chock full of them and it seems there are billboard ads for them every few miles along our highways. Add to this the fact that electronic banks are popping up everywhere on the Internet and you can conclude that the market seems to be very hot. Couple this with the fact that interest rates are ridiculously low for every bank and you wonder what keeps a customer with their existing bank if another offers a better deal or better service.

Credit card companies constantly send me incentives to get their cards. I have been offered platinum cards, diamond cards, gold cards, free gas, free long-distance, free grocery shopping, free miles, free cash back; credit limits from $20,000 to $100,000, 2.9% interest, 3.9% interest - where does the madness end?

You'd think the largest of the large financial institutions would have this customer service problem licked. They should be models of perfection. They should make sure that under no circumstances would they lose a customer to poor service. These institutions have millions of customers and advertising budgets in the tens of millions of dollars to attract new customers. If they didn't have great customer service, every day a smaller, nimbler competitor would be chasing their prime customers, stealing revenue from their pockets and bread from their tables. This is what I always thought, but boy was I naive.

In the last few months, I have witnessed customer service atrocities that would make me cringe if they came from my company. You wonder if executives in these large financial institutions ever try calling their own customer service lines themselves to see what the average customer has to suffer through.

Case in point is my recent need to acquire a mortgage for a house. After some shopping around, I decided to do business with the company that has also been handling my primary credit card. This is one of the largest banks in the country. When filling out my application and speaking with the representative from the mortgage company I mentioned I had a credit card with the same bank. This had absolutely no effect on cutting down my paperwork. I was a new customer and that was all there was to it - I had no credit history with them, they did not know me from Adam. I was a stranger. My credit card has been with this company for over ten years, yet I wasn't even in the computer. I mentioned my loyalty but no one cared.

Well, I got the mortgage and all was well for a few months until I realized I needed my credit limit extended on my credit card. So I called the credit card telephone number and told them that I needed my credit limit increased. After a week I received a letter informing me that I would need to send in a copy of my paycheck or a letter from my boss stating how much money I make. I called to tell them that my salary information, in fact my

entire life story, was in the mortgage department's computers. I mentioned to the customer service rep that the mortgage department could tell him how many square feet my house has, how many bathrooms, the year it was built; they know my lawyer, they know my accountant, and they even pay my property taxes for me - who knows me better? "I'm sorry sir, it doesn't work like that," I was told politely. "But why not?" I insisted. "Well, you see sir, the mortgage department works on a different computer system than the credit card department and we can't access their information and they can't access our information," he replied, being ever so polite. "Well great, I have their phone number, would you like to call them and double-check the figures I gave you?" I explained, hoping to ruffle the agent's feathers a bit. "Mr. Tehrani (now that he used my name I could tell I was getting to him), our corporate policy maintains that the credit limit adjustment department (or some such arcanely named department) must have the document faxed or mailed to us for recordkeeping purposes," he said in an agitated tone. I decided I had better things to do at this point than argue on the phone when I knew I was getting nowhere. I figured if "record-keeping purposes" were really that important, they would actually share some of these records with their other internal departments. Who needs these records? Are the agents getting commission on the number of records they save up? Are the agents archiving records in the computer in competition with each other? A brief flash of squirrel-like agents busily burying nuts in the yard flashed through my head. Well, I lost too much work time on this; I needed to get back to my job.

After a month or so, I forgot all about this encounter. I seem to be on the road more and more these days, and nothing clears my mind and helps me forget my problems like spending hours in an airplane. Thankfully, all my traveling has added up to a wealth of frequent flyer miles.

Frequent flyer miles equate to nobility in airports. I have hundreds of thousands of miles on certain airlines and merely thousands on others. If I fly airline X, I am a traveling god - my mere presence flying standby immediately reduces all other standby passengers in rank. I check in at certain "no wait" lines at airports. Life is good when I fly airline X.

Airline Y however, is different. When I fly this airline it seems to be for short hops. I can never **accumulate** the **miles** I need to reach the next level of flying status. Once, airline Y made me wait in an airport for 12 hours before I could fly out of the city - I was bumped off 6 standby lists. Recently, when I saw an ad offering a credit card yielding free **frequent flyer** miles on airline Y, I jumped at the chance. I had visions of reigning as an airport god on this airline as well. Better yet, the **credit** card **company** was the same **company** that offered my secondary **credit** card.

I immediately called the number on the screen and was barraged by questions: Name, age, social security number, etc. I mentioned I already had a card from this company but the agent, although pleasant, seemed unfazed. So I continued for a while until the agent finished the queries and I went back to watching TV.

A few days later, a letter came to my attention telling me that I must submit employment verification. So I found a pay stub and looked for the fax number on the enclosed letter. No fax number? In this day and age? I am impatient am I supposed to wait another week just for them to get to opening my letter? So I called and asked for the fax number. It turned out this bank didn't seem to have the same "record keeping" system as the last bank. In this case, only a letter will do. Here we go again. So I patiently explained that I have been a cardmember in good standing for over 12 years.

He said, "Oh, Mr. Tehrani, I did not realize this. Please give me your social security number again." Progress, I thought, progress. So I iterated the magic number and, lo and behold, my prior history was revealed to the agent and I no longer needed to submit anything. I hung up satisfied, but my subconscious didn't rest. I thought to myself that if the social security number is a unique identifier, why didn't I get picked up as a long-time customer already. I needed to tell the agent and the company that I am in their computer? This whole situation wasted time, paper, postage and telephone charges. We could have avoided all of this with a simple database query.

Based on these experiences, I know we are still in the nascent stages of a wonderful technology revolution in the call center. These above cases are ridiculous. A small company should be embarrassed, let alone a large company or the hugest of the huge, knowing that this sort of thing takes place in their call centers.

Perhaps you are thinking about your own call center. Do you have these

issues brewing? Are your databases in synch? Do they cross-reference and communicate with each other? Do you have call center software designed to catch this sort of problem?

I have issued a challenge. I have picked some of the major companies in the call center industry and presented them with the challenge of solving the above problems. I have asked for the products they would suggest and how they can link together to make sure the above scenarios never happen in your company. Our October issue of COLL CENTER Solutions(TM) will have a mini-round-up of companies that can tackle this challenge. Please be sure to read it thoroughly so you will ensure your company serves its customers as well as possible.

These types of scenarios remind me of the days when agents used 3 x 5 cards to keep track of their accounts. Call center software vendors have barely scratched the surface -- every company needs to make sure its call center data is accessible as needed by all other departments that have outside contact. People are busy and they are getting busier. Every call center must look at the latest products that will be outlined in the next issue and beyond.

To those banks in question: I noticed you subscribe to CM TM It seems to me you may not be reading as carefully as you need to be. Might I suggest that you take these challenges seriously before I or someone else decides to name you in future articles?

Sincerely yours,

Author Affiliation:

Rich Tehrani Group Publisher rtehrani@tmcnet.com

...TEXT: When I fly this airline it seems to be for short hops. I can never **accumulate** the **miles** I need to reach the next level of flying status. Once, airline Y made me...

...6 standby lists. Recently, when I saw an ad offering a credit card yielding free **frequent flyer** miles on airline Y, I jumped at the chance. I had visions of reigning as an airport god on this airline as well. Better yet, the **credit** card **company** was the same **company** that

offered my secondary **credit** card.

I immediately called the number on the screen and was barraged by questions: Name...

5/9,K/2 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

02393444 Supplier Number: 44730009 (THIS IS THE FULLTEXT)
Enter VeriFone
POS News, pN/A
June 1, 1994
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 715
TEXT:
Though Verifact's and Diebold's products may have their place at the table, the most notable advance for restaurant debit came last month from Redwood City, Calif.-based VeriFone Inc., the nation's largest terminal maker. VeriFone unveiled its Folio portable restaurant terminal at the National Restaurant Show in Chicago. VeriFone's terminal, which is about the size, shape and appearance of a waiter's order book and weighs about 20 ounces, was designed to look lean and sleek compared to Verifact's boxlike Spirit and to fit in the pocket of a server's apron. The unit looks like a calculator and the diner receives it from the server already programmed with the amount of the bill. The diner pays by inserting a credit or debit card, entering the PIN if required, entering or choosing a preset tip, and handing it back to the server. The server drops the Folio into a "docking station," a conduit through which transaction data enters the terminal for authorization. The market for such a device, if not here now, will materialize in time, VeriFone executives say. "My perception is consumers are slowly going to adapt to debit the same way they did to credit, and as they do it will permeate to other environments," says Michael Shade, director of VeriFone marketing programs and planning. "We will see the same thing slowly encroach into the restaurant world." Executives at all hardware vendors use words such as "slowly" to predict the spread of table-top debit to restaurants, but they insist an embryonic demand is there. The demand is rooted in consumer pressure: Just as supermarkets have adopted debit without a certainty of profitability and sometimes out of fear that customers will stray elsewhere, this could happen among leading restaurant chains seeking to ride the wave of modern trends. "They (sit-down restaurants) beat each other's brains out for business," Shade says. "So they're going to see this as a competitive opportunity." Manufacturers of restaurant debit terminals say that the devices offer restaurateurs several genuine advantages: improved convenience for diners that could translate into customer loyalty; reduced credit card discount fees; lower cash handling expenses, and easier settlement of tips because immediate debiting of tips by the customer eliminates the need to reprocess all checks overnight to compensate for gratuities. Even if restaurants don't have an interest in debit now, the terminal makers still hope their products sell as credit card terminals. But it is the device's capacity to do debit that will convince restaurant owners to try the terminals, even if they are not accepting debit now, in order to prepare for the future, Shade says. The targets for table-top debit are young card users who are already heavy users of plastic and who are using the card for leisure time and family dining. The likelihood that business diners would use a **company credit** card could limit the technology's appeal, Shade admits. "That could be a hindrance," he says. "We will all learn as we march ahead." The Folio

car companies, hotels, banks, **credit** or debit card issuers, telephone or other communication **company** , etc.

The consumer wishes to redeem these points to receive free airline tickets, meals, car...

```
? s (corporate (5n) frequent (5n) flyer) (10n) program (s) (miles or mileage)
Processing
Processed 10 of 26 files ...
Completed processing all files
9525043 CORPORATE
707025 FREQUENT
118902 FLYER
8783523 PROGRAM
1614524 MILES
122191 MILEAGE
S6 50 (CORPORATE (5N) FREQUENT (5N) FLYER) (10N) PROGRAM (S)
(MILES OR MILEAGE)
? rd s6

>>>Duplicate detection is not supported for File 348.

>>>Duplicate detection is not supported for File 349.

>>>Duplicate detection is not supported for File 347.

>>>Records from unsupported files will be retained in the RD set.
S7 23 RD S6 (unique items)
? s s7 and py<2001
Processing
Processed 10 of 26 files ...
Processing
Processed 20 of 26 files ...
Completed processing all files
23 S7
73938709 PY<2001
S8 18 S7 AND PY<2001
? t s8/3,k/1-18
```

8/3,K/1 (Item 1 from file: 9)
DIALOG(R)File 9:Business & Industry(R)
(c) 2006 The Gale Group. All rts. reserv.

01490944 Supplier Number: 24182056
Lan Chile invierte en beneficios
(Lan Chile will launch a frequent flyer program, Lan Pass, in 4/98)
El Diario, p 11
February 26, 1998
DOCUMENT TYPE: Business Newspaper (Chile)
LANGUAGE: Spanish RECORD TYPE: Abstract

ABSTRACT:
...Lan Chile, will begin one of its steps in its process of creating a new **corporate** image when the airline launches its overhauled **frequent flyer program** , Lan Pass, this April. Lan Chile has worked for the past year on making modifications...

...program to make it more competitive. The new system will allow frequent fliers to bank **miles** and not lose them if they have flown in the last two years, use accumulated **miles** for promotions with Lan Chile or associate airlines like American and Canadian Airlines, and accumulate **miles** for

stays with participating hotels. In June Lan Chile will incorporate Ladeco's Pass Club...

8/3,K/2 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

03660343 Supplier Number: 47883177 (USE FORMAT 7 FOR FULLTEXT)
Asiana 'On Target' to Become One of the 'World's Best Airlines'
World Airline News, v7, n31, pN/A
August 1, 1997
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 712

... both seat pitch and recline. To further attract premium travelers, the carrier established a special **frequent flyer program** for **corporate** accounts whereby Asiana awards **miles** to both the corporation and the traveling individual for the same trip.
The bid to...
19970801

8/3,K/3 (Item 1 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01887820 Supplier Number: 54768083 (USE FORMAT 7 FOR FULLTEXT)
www.continental.com Gets a Face-Lift; New Website Further Enhances Quick and Easy E-Commerce Experience.
PR Newswire, p0907
June 1, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 371

... has been reorganized to provide immediate access to flight information, E-tickets and OnePass bonus **miles** . These functions were moved up-front to expedite routine on-line transactions. For navigational purposes, Continental's website has five new areas for easy access: Business Travel Center, Vacations & Specials, **Frequent Flyer Program** , Travel Information & Services, and **Corporate** Information.
In addition to the face-lift, effective June 2, Continental Airlines is providing customers...
19990601

8/3,K/4 (Item 2 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01543116 Supplier Number: 47471304 (USE FORMAT 7 FOR FULLTEXT)
Continental Airlines Launches New York Campaign
PR Newswire, p0617DATU026
June 17, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 515

... J.D. Power and Associates Award for customer satisfaction as Best Airline for Flights 500 **miles** and more twice in a row. Other recent accolades include 1996 'Airline of the Year' by Air Transport World magazine and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** magazine.

SOURCE Continental Airlines

-0- 06/17/97
/CONTACT: **Corporate**
Communications, Continental Airlines, 713-834-5080/
(CAIB)

CO: Continental Airlines
ST: Texas, New York
IN...
19970617

8/3,K/5 (Item 3 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01517312 Supplier Number: 47290375 (USE FORMAT 7 FOR FULLTEXT)
Continental Airlines to Start New Flights to Honolulu and Nassau from Houston
PR Newswire, p0411DAF025
April 11, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 634

... by Air Transport World magazine, best airline in customer satisfaction for long-haul flights (500+ **miles**) by J.D. Power and Associates and **Frequent Flyer** magazine, and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** magazine.

SOURCE Continental Airlines

-0- 04/11/97
/CONTACT: **Corporate**
Communications of Continental Airlines, 713-834
-5080/
(CAI.B CAI.A)

CO: Continental Airlines
ST...
19970411

8/3,K/6 (Item 4 from file: 621)

DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01515579 Supplier Number: 47282891 (USE FORMAT 7 FOR FULLTEXT)
Continental Airlines and Colgan Air Sign Code-Share Agreement
PR Newswire, p0408DATU017
April 8, 1997
Language: English Record Type: Fulltext

Document Type: Newswire; Trade
Word Count: 382

... by Air Transport World magazine, best airline in customer satisfaction for long-haul flights (500+ **miles**) by J.D. Power and Associates and **Frequent Flyer** magazine, and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** magazine.

SOURCE Continental Airlines

-0- 4/8/97
/CONTACT: **Corporate** Communications of Continental Airlines, 713-834-5080; or Mary Finnigan of Colgan Air, 703-331...
19970408

8/3,K/7 (Item 5 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01506336 Supplier Number: 47224580 (USE FORMAT 7 FOR FULLTEXT)
Continental Airlines to Start New Service to Vancouver, British Columbia From Houston
PR Newswire, p0319DAW020
March 19, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 331

... by Air Transport World magazine, best airline in customer satisfaction for long-haul flights (500+ **miles**) by J.D. Power and Associates and **Frequent Flyer** magazine, and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** magazine.

SOURCE Continental Airlines, Inc.

-0- 3/19/97
/CONTACT: **Corporate** Communications of Continental Airlines, 713-834-5080/

(CAI.A CAI.B)

CO: Continental Airlines, Inc...
19970319

8/3,K/8 (Item 6 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01504200 Supplier Number: 47210681 (USE FORMAT 7 FOR FULLTEXT)
Continental Airlines Breaks Ground on Major Improvement Projects at IAH
PR Newswire, p0314DAF008
March 14, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 396

... by Air Transport World magazine, best airline in customer satisfaction for long-haul flights (500+ **miles**) by J. D. Power and

Associates and **Frequent Flyer** magazine and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** Magazine.

SOURCE Continental Airlines

-0- 3/14/97
/CONTACT: **CORPORATE** COMMUNICATIONS of Continental Airlines, 713-834-5080/

(CAI)

CO: Continental Airlines, Inc., Virgin Atlantic Airways...
19970314

8/3,K/9 (Item 7 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01503614 Supplier Number: 47207453 (USE FORMAT 7 FOR FULLTEXT)
Continental Airlines and Virgin Atlantic Airways Announce Code Share Arrangement
PR Newswire, p0313DATH021
March 13, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 630

... by Air Transport World magazine, best airline in customer satisfaction for long-haul flights (500 **miles** or more) by J. D. Power and Associates and **Frequent Flyer** Magazine and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** Magazine.

SOURCE Continental Airlines, Inc.

-0- 3/13/97
/CONTACT: **Corporate** Communications of Continental Airlines, Inc., 713-834-5080, or Will Whitehorn, (U.K.) 011-44...
19970313

8/3,K/10 (Item 8 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01490643 Supplier Number: 47127745 (USE FORMAT 7 FOR FULLTEXT)
Continental Airlines Pays $68 Million in Profit-Sharing Checks to Employees
PR Newswire, p214DAF002
Feb 14, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 457

... 1996, Continental Airlines was named best airline in customer satisfaction for long-haul flights (500+ **miles** or more) by J.D. Power and **Frequent Flyer** Magazine and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** magazine.

SOURCE Continental Airlines

-0- 2/14/97
/CONTACT: **Corporate**
Communications, Continental Airlines, 713-834-5080/
(CAI.A CAI.B)

CO: Continental Airlines
ST: Texas...
19970214

8/3,K/11 (Item 9 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01457358 Supplier Number: 46909953 (USE FORMAT 7 FOR FULLTEXT)
Alamo Adds Extra Frequent Flyer Rewards To Program For Corporate Customers
PR Newswire, p1121FLTH016
Nov 21, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 367

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
FORT LAUDERDALE, Fla., Nov. 21 /PRNewswire/ -- Alamo Rent-A-Car, Inc. has added extra **Frequent Flyer** Rewards to its **Corporate** Rate **Program** 's basic benefits. **Corporate** travelers who rent a car for at least three days can double, triple or even quadruple their frequent flyer **miles** /flight credits, depending on the day of pickup. All of Alamo's Airline partners are...
19961121

8/3,K/12 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

07124950 Supplier Number: 59419860 (USE FORMAT 7 FOR FULLTEXT)
EMPLOYEE PERKS: Best workplaces are revealed;MFS, Russell among financial services firms on the list.
Williamson, Christine
Pensions & Investments, v28, p2
Feb 7, 2000
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1161

... gives away trips to extravagant locales, such as 10 days at the Ritz in Hawaii. **Frequent flyer miles** accumulated by the company for **corporate** travel and credit cards fuel the **program** , said Joseph J. Trainor, president of MFS Institutional Advisors Inc.
On extra-snowy Boston days...
20000207

8/3,K/13 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

09212003 SUPPLIER NUMBER: 18989550 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Alamo chief defends commission cut. (Alamo Rent A Car vice chairman Roger Ballou)
Dorsey, Jennifer
Travel Weekly, v55, n104, p23(2)
Dec 30, 1996
ISSN: 0041-2082 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 831 LINE COUNT: 00069

... a car for at least three days to double, triple or quadruple their frequent flyer **mileage** credits, depending on the day of pickup.
Ballou said research shows that, all things being...

19961230

8/3,K/14 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2006 The Gale Group. All rts. reserv.

07993358 SUPPLIER NUMBER: 16838227 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Travel Network: best publicity relations & best promotional campaigns: sales of over $5 million.(Focus: Travel Weekly Sixth Annual Achievement Awards)
Travel Weekly, v54, n38, pF18(2)
May 15, 1995
ISSN: 0041-2082 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1499 LINE COUNT: 00125

...ABSTRACT: best public relations and promotional campaigns. The agency's Matching Miles promotion, similar to a **frequent flyer program** or **corporate** rebates. Travelers can accumulate **miles** and be awarded in free airline coach tickets. The program is aimed at business travelers...

19950515

8/3,K/15 (Item 3 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2006 The Gale Group. All rts. reserv.

06106565 SUPPLIER NUMBER: 12425503 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Asiana Airlines launches corporate frequent flyer program. (Brief Article)
Lassiter, Eric
Travel Weekly, v51, n56, p41(1)
July 13, 1992
DOCUMENT TYPE: Brief Article ISSN: 0041-2082 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT
WORD COUNT: 401 LINE COUNT: 00033

TEXT:
...Airlines, a South Korean carrier, has become the third international airline known to offer a **corporate mileage program** , allowing businesses to accumulate and use **frequent flyer** credits in the same manner as individuals.
... known to offer corporate mileage programs are Japan Airlines and Lufthansa.
Both airlines started their **corporate frequent flyer** programs years ago.
Asiana's **mileage program** is being administered out of its Los Angeles office.

The carrier pays agents 25% commission...

19920713

8/3,K/16 (Item 4 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2006 The Gale Group. All rts. reserv.

06046576 SUPPLIER NUMBER: 12528088
Air Miles adds nine corporate **sponsors**. (frequent flyer program)
Aviation Daily, v309, n32, p279(1)
August 14, 1992
ISSN: 0193-4597 LANGUAGE: ENGLISH RECORD TYPE: CITATION

Air Miles adds nine corporate **sponsors**. (frequent flyer program)

19920814

8/3,K/17 (Item 5 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2006 The Gale Group. All rts. reserv.

02820084 SUPPLIER NUMBER: 04191685 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Frequent flyer programs: who should reap benefits? (Dun's Business Month Focus)
Glab, Jim
Dun's Business Month, v126, p74(2)
April, 1986
ISSN: 0279-3040 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 1604 LINE COUNT: 00124

... standard "individuals-only" program; the JAL Corporate Passbook, which permits a company to combine the **mileage** of all its travelers into a single account, with the resulting free tickets awarded to the corporation; and JAL Corporate **Mileage** Bank, in which both individuals and their corporate employer can earn free tickets based on **mileage** . Since the programs were introduced about a year ago, some 250 companies

have joined the Passbook plan and more than 100 have signed up for the **Mileage** Bank.
Even if some airlines don't permit their awards coupons to be transferred, it...

19860400

8/3,K/18 (Item 1 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter
(c) 2006 Dialog. All rts. reserv.

09717901 (USE FORMAT 7 OR 9 FOR FULLTEXT)
EMPLOYEE PERKS: Best workplaces are revealed
Christine Williamson
PENSIONS & INVESTMENTS, p2
February 07, 2000
JOURNAL CODE: WCPI LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 1172

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... gives away trips to extravagant locales, such as 10 days at the Ritz in Hawaii. **Frequent flyer miles** accumulated by the company for **corporate** travel and credit cards fuel the **program** , said Joseph J. Trainor, president of MFS Institutional Advisors Inc.
On extra-snowy Boston days...

20000207
? ds

Set Items Description
S1 0 (FREQUENT ADJ5 FLIER)(S) (CREDIT?) (10N) (ORGANIZATION OR - CORPORATION OR COMPANY)
S2 786 (FREQUENT (5N) FLYER)(S) (CREDIT?) (10N) (ORGANIZATION OR CORPORATION OR COMPANY)
S3 0 S2 (S) ((DATA (1W)BASE) OR DATABASE)(5N) (EMPLOYEE)
S4 16 S2 (S) (ACCUMULAT?) (10N) (MILEAGE OR MILES)
S5 11 S4 AND PY<2001
S6 50 (CORPORATE (5N) FREQUENT (5N) FLYER) (10N) PROGRAM (S) (MI- LES OR MILEAGE)
S7 23 RD S6 (unique items)
S8 18 S7 AND PY<2001
? t s8/9,k/1-18

8/9,K/1 (Item 1 from file: 9)
DIALOG(R)File 9:Business & Industry(R)

01490944 Supplier Number: 24182056
Lan Chile invierte en beneficios
(Lan Chile will launch a frequent flyer program, Lan Pass, in 4/98)
El Diario, p 11
February 26, 1998
DOCUMENT TYPE: Business Newspaper (Chile)
LANGUAGE: Spanish RECORD TYPE: Abstract

ABSTRACT:
Chile's leading airline, Lan Chile, will begin one of its steps in its process of creating a new **corporate** image when the airline launches its overhauled **frequent flyer program** , Lan Pass, this April. Lan Chile has worked for the past year on making modifications to the Lan Pass program to make it more competitive. The new system will allow frequent fliers to bank **miles** and not lose them if they have flown in the last two years, use accumulated **miles** for promotions with Lan Chile or associate airlines like American and Canadian Airlines, and accumulate **miles** for stays with participating hotels. In June Lan Chile will incorporate Ladeco's Pass Club program into the Lan Pass program. The airline projects that by 2001 they will have 50 percent of their clients enrolled in the Lan Pass program.
COMPANY NAMES: LANCHILE
INDUSTRY NAMES: Airline; Transportation; Travel & leisure
PRODUCT NAMES: Air passenger carriers, scheduled (451282)
CONCEPT TERMS: All company; All market information; Corporate strategy; Marketing campaign
MARKETING TERMS: All product marketing; Loyalty
GEOGRAPHIC NAMES: Chile (CHL); Latin America (LAMX); South & Central America (SOCX)

ABSTRACT:

...Lan Chile, will begin one of its steps in its process of creating a new **corporate** image when the airline launches its overhauled **frequent flyer program** , Lan Pass, this April. Lan Chile has worked for the past year on making modifications...

...program to make it more competitive. The new system will allow frequent fliers to bank **miles** and not lose them if they have flown in the last two years, use accumulated **miles** for promotions with Lan Chile or associate airlines like American and Canadian Airlines, and accumulate **miles** for stays with participating hotels. In June Lan Chile will incorporate Ladeco's Pass Club...

8/9,K/2 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

03660343 Supplier Number: 47883177 (THIS IS THE FULLTEXT)
Asiana 'On Target' to Become One of the 'World's Best Airlines'
World Airline News, v7, n31, pN/A
August 1, 1997
ISSN: 1059-4183
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 712
TEXT:
In the ongoing rivalry between Korean Air and Asiana, the battle gottougher this week as Asiana took delivery of its 50th aircraft and published new fares -- as low as $699 roundtrip -- between the U.S. West Coast and Asia. The moves are part of numerous initiatives to seize a greater market share and become "one of the world's best airlines" by 2000. Asiana also aims to become one of the 20 largest airlines in terms of revenues by 2005. This year, it already is "ahead of schedule" in reaching its $1.7 billion revenue goal. Last year's revenues were $1.4 billion, up from $1.2 billion in 1995.
To fuel its efforts, the carrier is taking a hard look at codeshare partners but Patrick Khoury, Asiana's general manager marketing and sales for the Americas, said the airline has no plans to replicate the Star Alliance. Asiana currently has partnerships with Northwest Airlines [NWAC] (which just strengthened its relationship with KLM and said it is looking for other partners to join them), Qantas, Austrian Airlines, Air China, and China Eastern.
The Korean airline also is adding aircraft to its fleet at a furious pace: by 2005, its fleet will double to 100 aircraft, including 20 747-400s, 15 777s and 15 767s.
In May, Asiana launched an overhauled premium class product. It reduced the number of first class seats from 16 to 12 and is now one of the few carriers in the Pacific to offer the sleeper seat. In business class, Asiana reduced the number of seats from 36 to 32 to increase both seat pitch and recline. To further attract premium travelers, the carrier established a special **frequent flyer program** for **corporate** accounts whereby Asiana awards **miles** to both the corporation and the traveling individual for the same trip.
The bid to move up the global aviation ladder also goes beyond inflight service and new planes. Each department has been charged with specific goals to improve Asiana's product. At least one industry expert feels its efforts are paying off. "The overall impression I've been getting from people is that Asiana is offering better service [than Korean Air]," said Zayong Koo, an analyst with Clarion Securities in Hong Kong. "All in all, they've come a long way."

For continued growth, the carrier is most focused on the Asia/Pacific region, said Khoury, noting that the carrier also is taking a serious look at the Latin American and U.S. markets. In the U.S., Asiana's partnership with Northwest likely will play a greater role should the U.S. and Korea reach an open skies agreement. While Asiana will "obviously look at increasing frequencies," he said, "if codesharing is available and we would put our codes on our partners' aircraft."

Fortunes Likely to Head Up

Despite its ambitious plans, Asiana, which began service in 1988, faces some challenges both domestically and internationally. In the domestic market, the carrier has been plagued with a near-constant 30 percent market share since 1990, despite the Korean market's growth of almost 20 percent per year. Airline officials, however, are optimistic that they can achieve parity with their rival as they receive new aircraft. "Our ability to sustain increased market share will be commensurate with our fleet growth," said Khoury.

Still, Koo doubts that equality will be achieved soon. "I don't think [50-50 domestic market share] is possible in the next three to five years. That's not to say they won't be able to overcome Korean Air [in the long run]. With new aircraft, there will be a bit of overcapacity in both the domestic and international markets."

On the international side, Koo said the carrier has been gaining market share by taking it from foreign airlines rather than from Korean Air, but its emphasis on inflight service could reverse that trend. "They could now start slowly taking market share away from Korean Air if Korean Air doesn't improve its service and its amenities on board," Koo concluded.

*

Dispatch Reliability and On-Time Performance Were Well Above Average in 1996

Nonetheless, the carrier is aiming for 100 percent in both categories this year

Target Performance

Operation Frequency

International 99.9% 99.9%

Domestic 98.5% 96.0%

On-Time Frequency

International 90.0% 84.9%

Domestic 96.5% 94.9%

PUBLISHER NAME: Phillips Business Information, Inc.
COMPANY NAMES: *Asiana Airlines; Korean Air Lines Company Ltd. (Korea)
EVENT NAMES: *240 (Marketing procedures)
GEOGRAPHIC NAMES: *9SOUT (South Korea)
PRODUCT NAMES: *4510000 (Scheduled Airlines)
INDUSTRY NAMES: ADV (Advertising, Marketing and Public Relations); AERO (Aerospace and Defense); BUSN (Any type of business); INTL (Business, International); TRVL (Travel and Hospitality)
NAICS CODES: 4811 (Scheduled Air Transportation)

... both seat pitch and recline. To further attract premium travelers, the carrier established a special **frequent flyer program** for **corporate** accounts whereby Asiana awards **miles** to both the corporation and the traveling individual for the same trip.
The bid to...
19970801

8/9,K/3 (Item 1 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01887820 Supplier Number: 54768083 (THIS IS THE FULLTEXT)
www.continental.com Gets a Face-Lift; New Website Further Enhances Quick and Easy E-Commerce Experience.
PR Newswire, p0907
June 1, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 371
TEXT:
HOUSTON, June 1 /PRNewswire/ -- Continental Airlines (NYSE: CAL and CAL.A) today unveils its newly revamped website at www.continental.com. The site, recently ranked No. 1 again for customer satisfaction and loyalty by NPD, one of the largest marketing research firms in the U.S., has been completely redesigned to make it even more user-friendly and easier to navigate.
Responding to feedback from on-line users, www.continental.com features enhanced computer graphics and navigational aids that make it simpler and faster for travelers to purchase tickets and retrieve travel-related information on-line.
For example, the new homepage has been reorganized to provide immediate access to flight information, E-tickets and OnePass bonus **miles**

. These functions were moved up-front to expedite routine on-line transactions. For navigational purposes, Continental's website has five new areas for easy access: Business Travel Center, Vacations & Specials, **Frequent Flyer Program** , Travel Information & Services, and **Corporate** Information.
In addition to the face-lift, effective June 2, Continental Airlines is providing customers who come to the newly redesigned site valuable incentives, including an opportunity to receive 4,000 OnePass miles for purchasing a ticket with an American Express card.
"Our priority is to give customers a site tailored to their individual needs and by enhancing our site we've taken the first step toward Continental's global goal of putting the customer first in the on-line environment," said Steve Cossette, Continental's staff vice president, distribution planning.
Continental Airlines is the fifth largest airline in the U.S., offering more than 2,200 departures daily to 127 domestic and 79 international destinations. Operating major hubs in Newark, Houston and Cleveland, Continental (http://www.continental.com) has extensive service throughout the Americas, and to Europe and Asia. Continental recently initiated a strategic global alliance with Northwest Airlines. Continental is in the top half of FORTUNE magazine's "100 Best Companies to Work for in America," and has won first or second place in Frequent Flyer magazine and J.D. Power awards for four consecutive years. Continental has received numerous awards for its BusinessFirst premium cabin (Conde Nast Traveler, OAG Official Airline Guides, Entrepreneur and Smart Money magazines), OnePass frequent flyer program (InsideFlyer's Freddie Awards) and overall

operations and management (Air Transport World's 1997 Airline of the Year).

PUBLISHER NAME: PR Newswire Association, Inc.
COMPANY NAMES: *Continental Airlines Inc.
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *4510000 (Scheduled Airlines)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
SIC CODES: 4510 (Air Transportation, Scheduled, And Air Courier Services)
NAICS CODES: 4811 (Scheduled Air Transportation)

... has been reorganized to provide immediate access to flight information, E-tickets and OnePass bonus **miles** . These functions were moved up-front to expedite routine on-line transactions. For navigational purposes, Continental's website has five new areas for easy access: Business Travel Center, Vacations & Specials, **Frequent Flyer Program** , Travel Information & Services, and **Corporate** Information.
In addition to the face-lift, effective June 2, Continental Airlines is providing customers...
19990601

8/9,K/4 (Item 2 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01543116 Supplier Number: 47471304 (THIS IS THE FULLTEXT)
Continental Airlines Launches New York Campaign
PR Newswire, p0617DATU026
June 17, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 515
TEXT:
NEW YORK, June 17 /PRNewswire/ -- In an effort to capture a greater share of the world's largest airline market, Continental Airlines (NYSE: CAIB) is launching a new multi-million dollar campaign in the New York area today. It is the largest effort ever implemented to expand the awareness level of an airport anywhere in the world. A kickoff dinner tonight at Ellis Island for close to a thousand travel industry leaders will be hosted by Chairman and CEO Gordon Bethune.
Designed to "speak" to New Yorkers in their own voice, the campaign focuses almost exclusively on the benefits of the airline's hub at Newark International Airport and conveys to New Yorkers that Newark is closer and better than they think. Continental Airlines is the only carrier with a New York-area hub and offers more flights from the area than any other airline.
"What we're seeking to do is further penetrate the world's top airline market," said Bethune. "As the region's only hub airline, we know we can succeed."
The campaign, which includes radio, newspaper, direct mail and promotional events, has a heavy outdoor focus designed to be "graffiti-like" against urban backdrops such as pavement, brick, and construction walls. The sharp, witty, "in your face" copy includes lines like "Need to feel like a real New Yorker? Eat a bagel on your way to Newark," and "If you fly
Continental out of Newark raise your hand. The rest of you raise your standards." All lines end with the tag "Fly Continental Out of Newark." The radio spots feature the infamous New York City "taxi lady" voice extolling the benefits of Newark. Each begins with the standard "Please remember to take all of your belongings" message and quickly shifts to Continental.

"With this new campaign, Continental becomes part of the New York landscape while challenging people in a break-through, intriguing way, to change the way they think," said Bethune.
The campaign, created by New York based N.W. Ayer & Partners, will continue running through the end of 1997. Additional ads including new international service, new domestic routes and Frequent Flyer/J.D. Power-related messages will be added to the mix.
Continental Airlines is the fifth largest airline in the U.S., offering more than 2,000 jet and Express departures daily to 129 domestic and 59 international destinations. Operating major hubs in Newark, Houston, Guam and Cleveland, Continental is strategically positioned for transcontinental travel, and offers extensive service to Latin America and Europe via its Houston and Newark gateways. Recently, Continental became the only airline in history to earn the Frequent Flyer magazine/J.D. Power and Associates Award for customer satisfaction as Best Airline for Flights 500 **miles** and more twice in a row. Other recent accolades include 1996 'Airline of the Year' by Air Transport World magazine and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** magazine.

SOURCE Continental Airlines

-0- 06/17/97
/CONTACT: **Corporate**
Communications, Continental Airlines, 713-834-5080/
(CAIB)

CO: Continental Airlines
ST: Texas, New York
IN: AIR
SU: PDT

MS
-- DATU026 --
5527 06/17/97 15:21 EDT http://www.prnewswire.com

PUBLISHER NAME: PR Newswire Association, Inc.
COMPANY NAMES: *Continental Airlines Inc.
EVENT NAMES: *240 (Marketing procedures)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *4510000 (Scheduled Airlines)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
NAICS CODES: 4811 (Scheduled Air Transportation)

... J.D. Power and Associates Award for customer satisfaction as Best Airline for Flights 500 **miles** and more twice in a row. Other recent accolades include 1996 'Airline of the Year' by Air Transport World magazine and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** magazine.

SOURCE Continental Airlines

-0- 06/17/97
/CONTACT: **Corporate**
Communications, Continental Airlines, 713-834-5080/
(CAIB)

CO: Continental Airlines
ST: Texas, New York
IN...

8/9,K/5 (Item 3 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01517312 Supplier Number: 47290375 (THIS IS THE FULLTEXT)
Continental Airlines to Start New Flights to Honolulu and Nassau from Houston
PR Newswire, p0411DAF025
April 11, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 634
TEXT:
HOUSTON, April 11 /PRNewswire/ -- Continental Airlines (NYSE: CAI.B CAI.A) today announced new non-stop flights to Honolulu, Hawaii and Nassau, Bahamas from its Houston hub. Daily service to Honolulu begins Aug. 1. Nassau service starts June 26 and will initially operate twice weekly (Thursday and Sunday) and may eventually become a daily flight.
Continental is offering a low introductory fare of $498 round-trip for travel between Aug. 1 and Aug. 24. Deeper discounts are available between Aug. 25 and Nov. 20 ranging between $398 and $518 round-trip, depending on the day of travel. These fares apply only via the new non-stop Houston-Honolulu service. Tickets require an instant purchase, a minimum stay of three days, and reservations must be made 14 days prior to departure. The introductory sale ends April 30.
The Honolulu flight will leave Houston at 12:25 p.m. and arrive in Honolulu at 3:25 p.m. and continue on to Guam, Continental's hub in the Western Pacific. Flight time is approximately 8 hours. East Coast passengers traveling to Guam or other destinations in Micronesia will enjoy reduced travel time and elimination of a stop in California. The return flight will leave Honolulu at 9:30 p.m. and arrive in Houston at 9:50 a.m. the following day.
Continental will operate a 280-seat DC-10-30 featuring the airline's award-winning BusinessFirst service and regional cuisine by noted Hawaii chef and restaurateur Roy Yamaguchi.
"Our frequent flyers in Houston have been asking for non-stop service to Honolulu for some time, and we're pleased we can now offer them what they want," said Greg Brenneman, president and chief operating officer of Continental Airlines.
Continental currently operates two flights daily from the Mainland U.S. to Honolulu via Los Angeles and San Francisco. Its Pacific-based subsidiary, Continental Micronesia, provides daily service between Hawaii and both Japan and Micronesia.
Separately, Continental also announced plans to build the first and only wide-body aircraft maintenance hangar in Hawaii. The 112,000 square foot facility will be used to service Continental's Pacific fleet of B-747s and DC-10 aircraft. Construction is estimated at approximately $24 million. The hangar will be financed by Special Facility Revenue Bonds issued by the State of Hawaii with the sole responsibility of pay-back falling upon the airline. Construction should be completed by the Spring of 1998.
From April 12 - April 30, Continental is offering an introductory fare of $399 round-trip between Houston and Nassau. Travel must be completed by Aug. 31. Tickets require an instant purchase, a minimum stay of three days, and reservations must be made seven days prior to departure. This sales fare applies only via the new Houston-Nassau non-stop flight. The sale ends April 30.
Continental will operate a B-727 to Nassau, departing Houston at 2:30

p.m. and arriving in the Bahamas at 6:10 p.m. The return flight leaves Nassau at 11:35 a.m. and arrives Houston at 1:30 p.m.
Continental Airlines is the fifth largest airline in the U.S., offering more than 2,000 jet and Express departures daily to 129 domestic and 58 international destinations. Operating major hubs in Newark, Houston,

Guam and Cleveland, Continental is strategically positioned for transcontinental travel, and offers extensive service to Latin America and Europe via its Houston and Newark gateways. During 1996, Continental was named 'Airline of the Year' by Air Transport World magazine, best airline in customer satisfaction for long-haul flights (500+ **miles**) by J.D. Power and Associates and **Frequent Flyer** magazine, and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** magazine.

SOURCE Continental Airlines

-0- 04/11/97
/CONTACT: **Corporate**
Communications of Continental Airlines, 713-834
-5080/
(CAI.B CAI.A)

CO: Continental Airlines
ST: Texas
IN: AIR
SU:

JB
-- DAF025 --
9023 04/11/97 17:27 EDT http://www.prnewswire.com

PUBLISHER NAME: PR Newswire Association, Inc.
COMPANY NAMES: *Continental Airlines Inc.
EVENT NAMES: *360 (Services information)
GEOGRAPHIC NAMES: *1U9HI (Hawaii); 5BAHA (Bahamas)
PRODUCT NAMES: *4510000 (Scheduled Airlines)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
NAICS CODES: 4811 (Scheduled Air Transportation)
TRADE NAMES: 45100

... by Air Transport World magazine, best airline in customer satisfaction for long-haul flights (500+ **miles**) by J.D. Power and Associates and **Frequent Flyer** magazine, and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** magazine.

SOURCE Continental Airlines

-0- 04/11/97
/CONTACT: **Corporate**
Communications of Continental Airlines, 713-834
-5080/
(CAI.B CAI.A)

CO: Continental Airlines
ST...
19970411

8/9,K/6 (Item 4 from file: 621)

01515579 Supplier Number: 47282891 (THIS IS THE FULLTEXT)

Continental Airlines and Colgan Air Sign Code-Share Agreement

PR Newswire, p0408DATU017
April 8, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 382

TEXT:

HOUSTON, April 8 /PRNewswire/ -- Continental Airlines (NYSE: CAI.B CAI.A) today announced it has entered into a code-share agreement with Colgan Air, Inc. effective this summer on flights connecting in Boston, New York's La Guardia Airport, and Charlotte, NC.

Colgan Air will serve as a Continental Connection regional airline providing service throughout the Northeast and the Mid-Atlantic regions with over 60 flights daily. Under the terms of the agreement, Continental will handle all reservations for Colgan Air and all flights will appear as Continental flight numbers.

"This agreement allows Continental customers access to key Maine destinations, the historic and academic Charlottesville, VA areas, the West Virginia cities of Beckley and Bluefield, as well as the ever-popular vacation-oriented Hyannis and Nantucket, MA, with through check-in, competitive fares and accrual of OnePass frequent flyer mileage for the entire trip," said Tom Barber, Continental's vice president of alliance operations.

"We at Colgan Air are delighted to join Continental in this alliance. In combining the superior product offered by both our fine companies the customers will receive enormous benefits," said Charles J. Colgan, Colgan Air's president.

Colgan Air, Inc. is headquartered in Manassas, VA and provides service to nine states and 15 cities, operating a fleet of seven 19-passenger Beechcraft 1900s. The company, founded in 1991 by Colgan and his son Michael, operates hubs in New York La Guardia, Boston and Charlotte.

Continental Airlines is the fifth largest airline in the U.S., offering more than 2,000 jet and Express departures daily to 129 domestic and 58 international destinations. Operating major hubs in Newark, Houston, Guam and Cleveland, Continental is strategically positioned for transcontinental travel, and offers extensive service to Latin America and Europe via its Houston and Newark gateways. During 1996, Continental was named 'Airline of the Year' by Air Transport World magazine, best airline in customer satisfaction for long-haul flights (500+ **miles**) by J.D. Power and Associates and **Frequent Flyer** magazine, and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** magazine.

SOURCE Continental Airlines

-0- 4/8/97
/CONTACT: **Corporate** Communications of Continental Airlines, 713-834-5080; or Mary Finnigan of Colgan Air, 703-331-3102/
(CAI.B CAI.A) CO: Continental Airlines; Colgan Air, Inc. ST: Texas IN: AIR LEI SU:

JB
-- DATU017 --
9066 04/08/97 12:03 EDT http://www.prnewswire.com

PUBLISHER NAME: PR Newswire Association, Inc.

COMPANY NAMES: *Colgan Air Inc.; Continental Airlines Inc.
EVENT NAMES: *380 (Strategic alliances)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *4511010 (Domestic Air Passenger Svc)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
NAICS CODES: 481111 (Scheduled Passenger Air Transportation)

... by Air Transport World magazine, best airline in customer satisfaction for long-haul flights (500+ **miles**) by J.D. Power and Associates and **Frequent Flyer** magazine, and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** magazine.

SOURCE Continental Airlines

-0- 4/8/97
/CONTACT: **Corporate** Communications of Continental Airlines, 713-834-5080; or Mary Finnigan of Colgan Air, 703-331...
19970408

8/9,K/7 (Item 5 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01506336 Supplier Number: 47224580 (THIS IS THE FULLTEXT)
Continental Airlines to Start New Service to Vancouver, British Columbia From Houston
PR Newswire, p0319DAW020
March 19, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 331
TEXT:
HOUSTON, March 19 /PRNewswire/ -- Continental Airlines (NYSE: CAI.A CAI.B) today announced the airline will launch new non-stop service to Vancouver, British Columbia from its Houston hub June 12.
The flight will depart Houston at 10:00 a.m. and arrive in Vancouver at 12:46 p.m. The return flight from Vancouver will depart at 2:05 p.m. and will arrive in Houston at 8:36 p.m. The Vancouver flight will operate on a 128-seat Boeing 737 jet.
Connections from Vancouver to other destinations in Canada as well as Asia are readily available via Continental's code-share partner, Air Canada. The flight is also designed to provide easy transfers for passengers traveling on cruises from Vancouver.
"Continental's increased service to Canada in partnership with Air Canada represents the next phase in building connectivity between each of our respective networks," said David Grizzle, senior vice president of Alliance Development.
Continental intends on adding additional service from Houston to Vancouver and Toronto in 1998.
An introductory fare of $298 round trip, excluding taxes, is being offered for off-peak travel with tickets purchased by Mar. 25 and travel completed by Sept. 30.
Continental Airlines is the fifth largest airline in the U.S., offering more than 2,000 jet and Express departures daily to 131 domestic and 58 international destinations. Operating major hubs in Newark, Houston, Guam and Cleveland, Continental offers extensive service to Latin America and Europe via its New York/Newark and Houston gateways. During 1996, Continental was named 'Airline of the Year' by Air Transport World magazine, best airline in customer satisfaction for long-haul flights (500+

miles) by J.D. Power and Associates and **Frequent Flyer** magazine, and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** magazine.

SOURCE Continental Airlines, Inc.

-0- 3/19/97
/CONTACT: **Corporate** Communications of Continental Airlines, 713-834-5080/

(CAI.A CAI.B)

CO: Continental Airlines, Inc.
ST: Texas
IN: AIR
SU:

JB
-- DAW020 --
4565 03/19/97 11:16 EST http://www.prnewswire.com

PUBLISHER NAME: PR Newswire Association, Inc.
COMPANY NAMES: *Continental Airlines Inc.
EVENT NAMES: *360 (Services information)
GEOGRAPHIC NAMES: *1USA (United States); 1CBRI (British Columbia)
PRODUCT NAMES: *4510100 (Scheduled Air Passenger Svc)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
NAICS CODES: 481111 (Scheduled Passenger Air Transportation)
... by Air Transport World magazine, best airline in customer satisfaction for long-haul flights (500+ **miles**) by J.D. Power and Associates and **Frequent Flyer** magazine, and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** magazine.

SOURCE Continental Airlines, Inc.

-0- 3/19/97
/CONTACT: **Corporate** Communications of Continental Airlines, 713-834-5080/

(CAI.A CAI.B)

CO: Continental Airlines, Inc...
19970319

8/9,K/8 (Item 6 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01504200 Supplier Number: 47210681 (THIS IS THE FULLTEXT)
Continental Airlines Breaks Ground on Major Improvement Projects at IAH
PR Newswire, p0314DAF008
March 14, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 396
TEXT:
HOUSTON, March 14 /PRNewswire/ -- Continental Airlines (NYSE: CAI.B and CAI.A) kicked off $190 million in capital improvement projects at Houston Intercontinental Airport today. Construction commenced on a $70 million

renovation of Terminal B for new gates, ticket counters, baggage system, offices, support space, a second Presidents Club, and on 'TerminaLink,' a

$75 million automated people mover that will link Terminals B and C. In addition, Continental will break ground early this summer on a $15 million mail sort facility and a $30 million line maintenance facility. The terminal renovations, mail sort facility and line maintenance facility will be completed by the summer of 1998. The new 'TerminaLink' will be completed by the summer of 1999.

"These capital improvement projects are required for the successful growth of the Houston hub. We plan to add more flights to more destinations and grow our departures from 438 today to 525-550 over the next several years. The over 1,000 new jobs that will be created from this expansion would have not been possible without the assistance of Mayor Lanier and the City Council Aviation Committee. We are very grateful for this support," said Greg Brenneman, Continental Airlines president and chief operating officer.

In September, Continental Express will move its entire flight operation into Terminal B and begin flying its new 50-seat ExpressJet, the Brazilian-made Embraer 145. All ExpressJet flights will be jetbridge loaded from the passenger terminal. A bus will connect Continental Express passengers from B and C until the 'TerminaLink' is completed.

Continental is the fifth largest airline in the U.S., offering more than 2,000 jet and Express departures daily to 131 U.S. and 58 international destinations. Operating major hubs in Newark, Houston, Guam and Cleveland, Continental is strategically positioned for transcontinental travel, and offers extensive service to Latin America and Europe via its Houston and Newark gateways. During 1996, Continental was named 'Airline of the Year' by Air Transport World magazine, best airline in customer satisfaction for long-haul flights (500+ **miles**) by J. D. Power and Associates and **Frequent Flyer** magazine and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** Magazine.

SOURCE Continental Airlines

-0- 3/14/97
/CONTACT: **CORPORATE** COMMUNICATIONS of Continental Airlines, 713-834-5080/

(CAI)

CO: Continental Airlines, Inc., Virgin Atlantic Airways Limited
ST: Texas
IN: AIR
SU:

SW
-- DAF008 --
3501 03/14/97 11:05 EST http://www.prnewswire.com

PUBLISHER NAME: PR Newswire Association, Inc.
COMPANY NAMES: *Continental Airlines Inc.
EVENT NAMES: *250 (Financial management)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *4510000 (Scheduled Airlines)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
NAICS CODES: 4811 (Scheduled Air Transportation)
TRADE NAMES: 45100

... by Air Transport World magazine, best airline in customer satisfaction for long-haul flights (500+ **miles**) by J. D. Power and Associates and **Frequent Flyer** magazine and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** Magazine.

SOURCE Continental Airlines

-0- 3/14/97
/CONTACT: **CORPORATE** COMMUNICATIONS of Continental Airlines, 713-834-5080/

(CAI)

CO: Continental Airlines, Inc., Virgin Atlantic Airways...
19970314

8/9,K/9 (Item 7 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01503614 Supplier Number: 47207453 (THIS IS THE FULLTEXT)
Continental Airlines and Virgin Atlantic Airways Announce Code Share Arrangement
PR Newswire, p0313DATH021
March 13, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 630
TEXT:
NEWARK, Mar. 13 /PRNewswire/ -- Continental Airlines, Inc. (NYSE: CAI.B and CAI.A) and Virgin Atlantic Airways Limited announced today that they have signed a memorandum of understanding for a code share arrangement involving the carriers' Newark/New York-London routes and eight other routes between the United Kingdom and the United States. This arrangement will replace Virgin Atlantic's alliance with Delta Air Lines which will terminate later this year.
The arrangement, which will be subject to governmental approvals and certain documentation, contemplates the addition by Continental of two daily flights between Newark and London (bringing its daily number of Newark-London flights to four) and the addition of a second daily flight by Virgin Atlantic between London and Newark, as well as the carrier's two daily flights from London to JFK. Continental expects to add two DC10-30 aircraft to its Newark- London routes, and Virgin Atlantic expects to add an additional Boeing 747.
The carriers will exchange blocks of seats on all their Newark/New York-London routes, thereby giving Continental limited access to London's Heathrow Airport and giving each carrier the ability to sell seats on a wider frequency of services. Each carrier will sell, market and price its seats independently in competition with the other, thereby providing consumers with additional choice across the Atlantic.
In addition, Continental will purchase a block of seats for resale on Virgin Atlantic's daily flights between London and each of Boston, Washington-Dulles, Los Angeles (soon to be twice daily), Miami, Orlando, and San Francisco, and between Manchester and Orlando.
"We are delighted to welcome Virgin Atlantic Airways as a code share partner," said Gordon M. Bethune, Continental's chairman and chief executive officer. "Although this arrangement will give Continental limited access to Heathrow, it's nowhere near what we need to counter the juggernaut being proposed by British Airways and American Airlines. If that

anti-competitive transaction is approved, Continental alone will need at least 140 Heathrow slots even to begin to compete effectively."
Virgin Atlantic's Chairman, Richard Branson said, "Our new code share deal with Continental brings together two similar business philosophies based on quality of customer service and value for money. Both carriers will continue to bring the benefits of real competition to consumers on both sides of the Atlantic."
In just twelve years Virgin Atlantic has become the UK's second largest long-haul carrier of passengers and freight and has won virtually every award the industry has to offer. Flights operate from London to New York JFK, Newark, Boston, Washington, Los Angeles, San Francisco, Miami, Orlando, Tokyo, Hong Kong, Johannesburg and Athens.
Virgin Atlantic has taken delivery of a new Boeing 747-400 aircraft this month with a second due to arrive in early July. A further three

A340 aircraft will arrive in the second quarter of 1997.
Continental Airlines is the fifth largest airline in the U.S., offering more than 2,100 jet and Express departures daily to 131 domestic and 58 international destinations. Operating major hubs in Newark, Houston, Guam and Cleveland, Continental is strategically positioned for transcontinental travel, and offers extensive service to Latin America and Europe via its Houston and Newark gateways. During 1996, Continental Airlines was named 'Airline of the Year' by Air Transport World magazine, best airline in customer satisfaction for long-haul flights (500 **miles** or more) by J. D. Power and Associates and **Frequent Flyer** Magazine and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** Magazine.

SOURCE Continental Airlines, Inc.

-0- 3/13/97
/CONTACT: **Corporate** Communications of Continental Airlines, Inc., 713-834-5080, or Will Whitehorn, (U.K.) 011-44-171-229-4738, or Amy Curtis, (U.S.) 203-750-2570, both of Virgin Atlantic Airways/

(CAI.B, CAI.A)

CO: Continental Airlines, Inc., Virgin Atlantic Airways Limited
ST: Texas
IN: AIR
SU:

DG
-- DATH021 --
6634 03/13/97 12:52 EST http://www.prnewswire.com

PUBLISHER NAME: PR Newswire Association, Inc.
COMPANY NAMES: *Continental Airlines Inc.; Virgin Atlantic Airways Ltd.
EVENT NAMES: *380 (Strategic alliances)
GEOGRAPHIC NAMES: *1USA (United States); 4EUUK (United Kingdom)
PRODUCT NAMES: *4510000 (Scheduled Airlines)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
NAICS CODES: 4811 (Scheduled Air Transportation)

... by Air Transport World magazine, best airline in customer satisfaction for long-haul flights (500 **miles** or more) by J. D. Power and Associates and **Frequent Flyer** Magazine and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** Magazine.

SOURCE Continental Airlines, Inc.

-0- 3/13/97
/CONTACT: **Corporate** Communications of Continental Airlines, Inc., 713-834-5080, or Will Whitehorn, (U.K.) 011-44...
19970313

8/9,K/10 (Item 8 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01490643 Supplier Number: 47127745 (THIS IS THE FULLTEXT)
Continental Airlines Pays $68 Million in Profit-Sharing Checks to Employees
PR Newswire, p214DAF002
Feb 14, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 457
TEXT:
HOUSTON, Feb. 14 /PRNewswire/ -- Continental Airlines (NYSE: CAI.B and CAI.A) today began distributing 1996 profit-sharing checks to its 37,500 employees. By the end of the day the company will have paid out $68 million, representing approximately 7 percent of employees' annual wages. At kickoff events in Newark, Houston and Cleveland, Continental's senior management praised employees for the company's stellar performance in 1996, while personally handing out profit-sharing checks. Continental recently announced an all-time record annual pre-tax profit for 1996 of

$556 million excluding previously announced special charges, the second consecutive record- breaking year. The company also ended the year with a cash balance of more than $1 billion -- the highest in company history -- and finished in the top three in all four industry metrics, which contributed to it being named Airline of the Year by Air Transport World. "What a sweetheart day this is. Our employees deserve every penny of the $68 million -- they earned it," said Chairman and Chief Executive Officer Gordon Bethune.
Continental's profit-sharing plan pays 15 percent of pre-tax net income and is divided among eligible employees based on their salaries. Since the company's earnings were higher in 1996, this year's profit-sharing checks are double the amount paid out one year ago.
In addition, Continental has paid its employees $29 million in on-time bonuses for 1996 in keeping with the company's incentive performance program. Each month the carrier finished first in on-time performance, employees received $100, and they received $65 for second or third place. When combined with the 1996 profit-sharing, the company has shared more than $97 million with its workforce.
Continental's profit-sharing checks will generate a significant economic impact in many cities throughout the U.S. In anticipation, retail merchants in the airline's hub cities of Newark, Houston and Cleveland are offering Continental employees special discounts on purchases or allowing them special offers. Full-page ads are appearing in newspapers in these cities today.
Continental Airlines is the fifth largest airline in the U.S., offering more than 2,100 jet and Express departures daily to 131 domestic and 57 international destinations. Operating major hubs in Newark, Houston, Guam and Cleveland, Continental is strategically positioned for transcontinental travel, and offers extensive service to Latin America and Europe via its Houston and Newark gateways. During 1996, Continental Airlines was named best airline in customer satisfaction for long-haul flights (500+ **miles** or more) by J.D. Power and **Frequent Flyer**

Magazine and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** magazine.

SOURCE Continental Airlines

-0- 2/14/97
/CONTACT: **Corporate**
Communications, Continental Airlines, 713-834-5080/
(CAI.A CAI.B)

CO: Continental Airlines
ST: Texas, New Jersey, Ohio
IN: AIR
SU:

BS
-- DAF002 --
3193 02/14/97 09:30 EST http://www.prnewswire.com

PUBLISHER NAME: PR Newswire Association, Inc.
COMPANY NAMES: *Continental Airlines Inc.
EVENT NAMES: *830 (Sales, profits & dividends)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *4510000 (Scheduled Airlines)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
NAICS CODES: 4811 (Scheduled Air Transportation)

... 1996, Continental Airlines was named best airline in customer satisfaction for long-haul flights (500+ **miles** or more) by J.D. Power and **Frequent Flyer** Magazine and Best Elite-Level **Frequent Flyer Program** by Inside **Flyer** magazine.

SOURCE Continental Airlines

-0- 2/14/97
/CONTACT: **Corporate**
Communications, Continental Airlines, 713-834-5080/
(CAI.A CAI.B)

CO: Continental Airlines
ST: Texas...
19970214

8/9,K/11 (Item 9 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01457358 Supplier Number: 46909953 (THIS IS THE FULLTEXT)
Alamo Adds Extra Frequent Flyer Rewards To Program For Corporate Customers
PR Newswire, p1121FLTH016
Nov 21, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 367
TEXT:
FORT LAUDERDALE, Fla., Nov. 21 /PRNewswire/ -- Alamo Rent-A-Car, Inc. has added extra **Frequent Flyer** Rewards to its **Corporate** Rate **Program** 's basic benefits. **Corporate** travelers who rent a car for at least three

days can double, triple or even quadruple their frequent flyer **miles** /flight credits, depending on the day of pickup. All of Alamo's Airline partners are participating in this program for rentals reserved and rented in North America.
On corporate Rate Codes BX and BW, rentals for three days or more with pickup on Tuesday through Saturday, will receive extra frequent flyer miles/flight credits as follows:

Length of Rental Day of Pickup Number of FF Credits
3-7 days Tuesday-Saturday Double
8 + Tuesday-Saturday Triple
For corporate Rate Code BX only, renters can earn extra frequent flyer miles/flight credits on rentals of three days or longer with pickups on Sunday or Monday as follows:

Length of Rental Day of Pickup Number of FF Credits
3-7 days Sunday/Monday Triple
8 + Sunday/Monday Quadruple
"Alamo's objective is to be a major force in this important market segment. We plan to do that by focusing our Corporate Rate Program on the business and leisure needs of our corporate customers," said Fred Filippi, Alamo's vice president, commercial sales & marketing. "Offering the best value-added programs available in the industry today is our way of saying thank you for your business," added Filippi.
In addition to the extra Frequent Flyer Rewards, free enrollment in our Quicksilver(SM) express rental service and True Blue(SM) frequent renter program are automatically included in Alamo's Corporate Rate Program. A qualifying flight on participating airlines may be required. For more information, contact your Alamo Sales Representative or call Alamo at 800-882-5266.
Alamo currently serves more than 15 million travelers each year at 192 locations throughout the United States and Canada, and more than 160 locations internationally in the United Kingdom, Ireland, Switzerland, Belgium, The Netherlands, Germany, Greece, Portugal and the Czech Republic.

SOURCE Alamo Rent A Car

-0- 11/21/96

/CONTACT: April Fiur, Public Relations, Alamo Rent A Car, 954-468-2146
/

CO: Alamo Rent A Car
ST: Florida
IN: LEI
SU: PDT

RK
-- FLTH016 --
5462 11/21/96 13:57 EST http://www.prnewswire.com

PUBLISHER NAME: PR Newswire Association, Inc.
COMPANY NAMES: *Alamo Rent A Car Inc.
EVENT NAMES: *240 (Marketing procedures)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *7512000 (Automobile Rent & Lease)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)

NAICS CODES: 52311 (Investment Banking and Securities Dealing)

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
FORT LAUDERDALE, Fla., Nov. 21 /PRNewswire/ -- Alamo Rent-A-Car, Inc. has added extra **Frequent Flyer** Rewards to its **Corporate** Rate **Program** 's basic benefits. **Corporate** travelers who rent a car for at least three days can double, triple or even quadruple their frequent flyer **miles** /flight credits, depending on the day of pickup. All of Alamo's Airline partners are...
19961121

8/9,K/12 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

07124950 Supplier Number: 59419860 (THIS IS THE FULLTEXT)
EMPLOYEE PERKS: Best workplaces are revealed;MFS, Russell among financial services firms on the list.
Williamson, Christine
Pensions & Investments, v28, p2
Feb 7, 2000
ISSN: 1050-4974
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1161
TEXT:
From midafternoon basketball games to paid sabbaticals, the 13 financial services firms on Fortune's list of the 100 best places to work offer perks rarely seen in other investment management companies.
Among them:
* MFS Investment Management, Boston, sometimes halts afternoon meetings for staff basketball games.
* Charles Schwab & Co., San Francisco, and Frank Russell Co., Tacoma, Wash., give employees paid sabbaticals. Schwab also has a permanent dress code of "business casual" and provides a concierge service for employees.
* American Century Cos. Inc., Kansas City, Mo., offers domestic partner health benefits that let the employee define "family."
Companies ask to be included in the Fortune survey. Two-thirds of a firm's score is based on employee responses to a survey. The other third is based on Fortune's review of the company's materials. Hewitt Associates LLC, Lincolnshire, Ill., helped Fortune design and tabulate the survey.
Other money management-related firms on the list are: Janus Capital Corp., Denver; Northern Trust Corp., Chicago; American Express Financial Corp., Minneapolis; and Goldman, Sachs & Co., New York.
Randall K. Abbott, a senior consultant and practice leader in the Philadelphia office of Watson Wyatt Worldwide, an employee benefits consulting firm, said personalization and fun help companies market themselves as good places to work, in essence creating a brand identity in the employee's mind.
"I would be looking at the people in my organization who manage the most money, if I were a money manager. And I would pick 10 or 20 of them and think about what I could do to tie those people in even more closely, to retain them long term. There will be a different answer for each person, but this personalization, making people happy in the way they want it most, that's what will keep people at the company," Mr. Abbott said.
Here's what a few companies do for their employees:
MFS
MFS Chairman Jeff Shames loves basketball. Company business has been

known to cease in the middle of the afternoon, at least for some employees, who head off for pickup games with their boss.
And, when MFS passed the $100 billion mark last year for assets under management, every employee received a $100 bill.
MFS has a gala holiday party, where it gives away trips to extravagant locales, such as 10 days at the Ritz in Hawaii. **Frequent flyer miles** accumulated by the company for **corporate** travel and credit cards fuel the **program** , said Joseph J. Trainor, president of MFS Institutional Advisors Inc.
On extra-snowy Boston days, pizza often is brought in to keep employees happy and warm and, a few times a year, gallons of ice cream and liters of toppings are brought in for ice cream sundae parties. A fall harvest fair in an apple orchard brings families together for apple picking, a barbecue and hay rides and games, said Mr. Trainor.
Schwab
At Schwab, a player in the 401(k) marketplace, management believes

that in order to treat customers well, a company needs to treat its employees well, said Beth Sawi, chief administrative officer.
Beginning in April, employees with five years of service will be eligible for four-week paid sabbaticals that can be combined with vacation time. The sabbatical benefit increases to eight weeks after 10 years.
"Our employees work really hard and we want to make sure they get some R&R," she said.
Part of that excellent treatment recently included $100 American Express gift certificates, a way of thanking workers for a successful navigation of the tricky Y2K period, when vacation time was frozen.
Schwab also offers a concierge service that takes care of everything from finding theater tickets for out-of-town relatives to researching home contractors to helping with solutions to family problems.
"We want to make sure employees have all that they need to eliminate hassles in their lives so they can focus on work," Ms. Sawi said.
Schwab also rewards employees financially, she said. She cited a generous employee stock ownership program that has made 10% of Schwab employees into millionaires, as well as yearly cash performance bonuses, occasional options grants, spot bonuses and a generous 401(k) plan.
"We want employees to be financially tied to Schwab. We want them to know that profits aren't hoarded at the top," Ms. Sawi said.
Schwab also has a commitment to community service and volunteerism, including a big project with Habitat for Humanity. Its peer-nominated Schwab Volunteer of the Year is recognized at the company's annual meeting. The employee's charity of choice receives $5,000 from the company.
Frank Russell
Russell also has a senior exec who heads off on a regular basis to play afternoon basketball, part of a work-life balance program that pervades the whole company, said Craig Ueland, chief operating officer.
"People don't want to work just for money. They need to be motivated," he said.
It was Mr. Ueland who inspired Frank Russell to offer a sabbatical program -- eight paid weeks off every 10 years. He was returning to the United States after setting up Russell's Sydney, Australia, office and took a month off without pay to travel with his wife. It turned out to be such a rejuvenating experience that many others at Russell wanted to do the same thing. But Russell officials realized many employees couldn't afford a month without pay, so they instituted the paid sabbatical policy.
Russell folks are no slouches when it comes to community giving. Several Russell employees set up their own charitable foundations with the money they made when Frank Russell was acquired by Northwestern Mutual Life Insurance Co., Milwaukee, in 1998.
The Russell family is also a big benefactor throughout Tacoma, which

inspires many employees to contribute both time and money to charity causes, such as Habitat for Humanity and tutoring programs in local schools.
"We have a lot of tree-huggers in the company, outdoors people. It is part of their culture and the culture of the company to literally take care of our people and to take care of the community," Mr. Ueland said.
They take care of their own, too. Russell employees find a flower on their desks on their birthdays and employment anniversaries. And, a big company picnic every year at a local fairground brings families together.
American Century
American Century's founding family, the Stowers, also are benefactors in the company's home town. Employees follow suit: Overall, American Century employees contribute at least 4,500 hours of community service every year.
The company has been known to share the wealth during exceptionally good years. In 1997 and 1999, for example, every employee got an extra paycheck, said spokeswoman Julie Bartels Smith.
American Century also is one of just a few U.S. companies that offers domestic partner medical benefits that allow the employee to designate who -- besides a spouse -- is "family" and should receive medical coverage. The only requirement is that the individual has lived with the employee for at least a year. Some have designated a younger sibling, others an in-law, nanny or significant other.

PUBLISHER NAME: Crain Communications, Inc.
COMPANY NAMES: *Frank Russell Co.; American Century Companies Inc.; Charles Schwab and Company Inc.
EVENT NAMES: *280 (Personnel administration)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *6411000 (Insurance Agents & Brokers); 6211000 (Securities Dealers)
INDUSTRY NAMES: BANK (Banking, Finance and Accounting); BUSN (Any type of business); INSR (Insurance and Human Resources)
SIC CODES: 6411 (Insurance agents, brokers, & service); 6211 (Security brokers and dealers)
NAICS CODES: 52421 (Insurance Agencies and Brokerages); 52311 (Investment Banking and Securities Dealing)
TICKER SYMBOLS: ACT
SPECIAL FEATURES: LOB; COMPANY

... gives away trips to extravagant locales, such as 10 days at the Ritz in Hawaii. **Frequent flyer miles** accumulated by the company for **corporate** travel and credit cards fuel the **program** , said Joseph J. Trainor, president of MFS Institutional Advisors Inc.
On extra-snowy Boston days...
20000207

8/9,K/13 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

09212003 SUPPLIER NUMBER: 18989550 (THIS IS THE FULL TEXT)
Alamo chief defends commission cut. (Alamo Rent A Car vice chairman Roger Ballou)
Dorsey, Jennifer
Travel Weekly, v55, n104, p23(2)
Dec 30, 1996
ISSN: 0041-2082 LANGUAGE: English RECORD TYPE: Fulltext; Abstract

WORD COUNT: 831 LINE COUNT: 00069

ABSTRACT: Alamo Rent A Car has reduced its corporate rates to 5% from 10% as of Jan 1, 1997, just as other car rental companies did years ago. The company's leisure rates will continue to be 10%. Alamo plans to increase its corporate accounts, especially in small and midsized businesses. Smaller accounts are more lucrative than larger accounts.

TEXT:
FORT LAUDERDALE, Fla. - Alamo Rent A Car's decision to cut commissions on contracted corporate rates to 5% is by no means at odds with the company's efforts to build up corporate sales, according to Roger Ballou, Alamo's vice chairman and chief operating officer.
In a telephone interview, Ballou said that with the change in commission policy, "all we've done is match what everybody (else) has done years ago."
"We are absolutely very aggressively growing our corporate business, particularly focusing on small and midsize accounts," he said.
"With competitive commissions, it's a profitable market, and we can make some money on it."
As reported, Alamo announced that commissions on contracted corporate, association and government and military "on business" rates will change Jan. 1 from 10% to the "5% commission standard set by other major car rental companies."
Alamo said it will continue to pay 10% on all retail and promotional bookings for the leisure market, with periodic promotions offering higher commissions.
In addition, Ballou said that if a corporate client books a retail rate and provides a corporate ID number, the agent will earn 10% on that rate.
Overall, Alamo said in a press release, the commission change on the corporate side "will not affect the majority of travel agency bookings with Alamo."
"In addition, earning opportunities beyond the aggressive base commission structure include preferred account overrides, commission specials and frontline agent incentives, all (of) which play a key role in the overall agent compensation plan," Alamo said.
Ballou said, "Our position in the market is to try to give corporate clients, and agents' clients, rates that are more attractive than major competitors.'
"We found it was impossible to give better pricing and pay 5% more than anybody else was paying on the same business."
Ballou explained that, "in a business with a 5% margin, you have to generate a huge increase in volume to pay for giving an extra 5% commission."
"We just couldn't make money. (There is) no way to get enough preference out of agents to make money when you've got zero margin," he said.
Of the business that Alamo receives from travel agents, Ballou said that two-thirds to three-quarters is leisure bookings, where commissions have not changed.
On the corporate side, agents with fee-based pricing arrangements with their large accounts return rental car commissions to the clients, so the change in commission "makes no economic difference to them at all," he said.
As a result, Ballou said, "you get down to a very small percentage of our volume where this (commission reduction) would have an effect on the agent."
Predominantly leisure-oriented now, Alamo's goal is to have 40% of its business eventually consist of corporate bookings, Ballou said.

He declined to provide a time frame for achieving that goal, saying he would prefer not to give Alamo's competitors a blueprint of the company's plans.
Ballou described Alamo's corporate targets as small accounts, with less than $15,000 in annual rental car volume, and midsize accounts, with between $15,000 and $500,000.
Those accounts are more lucrative than the large ones because rates are slightly higher and because clients are "typically more focused on the value they get in the transaction," Ballou said.
"Our positioning is as the value leader."
In contrast, Ballou said, margins are lower on the large corporate accounts.
That business typically is handled in the form of megabids, and most large accounts have multiyear relationships with vendors that are longstanding and hard to break.
"It is a lower-margin business with a higher cost of entry," Ballou said.
Alamo's goal is to have roughly a 25% share of small-business accounts, up from a little less than 10% now, and 15% of the midsize accounts, up from roughly 5% now, Ballou said.
Frequent-traveler rewards are one tool being used by the company to capture a bigger share of both markets.
For example, Alamo recently added extra frequent flyer rewards to its corporate rate program's basic benefits, enabling corporate travelers who rent a car for at least three days to double, triple or quadruple their frequent flyer **mileage** credits, depending on the day of pickup.
Ballou said research shows that, all things being equal, frequent flyer benefits rank among the top three reasons for choosing one car rental

company over another.
Ballou said research also shows that with small corporate accounts in particular, the decision-maker - often one of the most frequent travelers - is the owner.
Frequent traveler benefits have "a lot more visceral appeal to those individuals," he said.
In Alamo's True Blue frequent renter program, which offers awards for free Alamo rentals, small-business owners can receive credits for the equivalent of all the points earned by their employees during the course of the year.

SPECIAL FEATURES: illustration; photograph
COMPANY NAMES: Alamo Rent A Car Inc.--Prices and rates
INDUSTRY CODES/NAMES: TRVL Travel and Hospitality; BUSN Any type of business
DESCRIPTORS: Automobile lease and rental industry--Prices and rates
PRODUCT/INDUSTRY NAMES: 7512000 (Automobile Rent & Lease)
SIC CODES: 7510 Automotive Rentals, No Drivers
FILE SEGMENT: TI File 148

... a car for at least three days to double, triple or quadruple their frequent flyer **mileage** credits, depending on the day of pickup.
Ballou said research shows that, all things being...

19961230

8/9,K/14 (Item 2 from file: 148)

07993358 SUPPLIER NUMBER: 16838227 (THIS IS THE FULL TEXT)
Travel Network: best publicity relations & best promotional campaigns: sales of over $5 million.(Focus: Travel Weekly Sixth Annual Achievement Awards)
Travel Weekly, v54, n38, pF18(2)
May 15, 1995
ISSN: 0041-2082 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1499 LINE COUNT: 00125

ABSTRACT: Travel Network, in Englewood Cliffs, NJ, has won the Travel Weekly's award for travel agency's with over $5 million with the best public relations and promotional campaigns. The agency's Matching Miles promotion, similar to a **frequent flyer program** or **corporate** rebates. Travelers can accumulate **miles** and be awarded in free airline coach tickets. The program is aimed at business travelers, and has been well publicized among the agency's franchises.

TEXT:
BEST PUBLIC RELATIONS & BEST PROMOTIONAL CAMPAIGNS: Sales of over $5 million
These are some examples of the enthusiastic comments that Matching Miles, a far-reaching promotion introduced last September by Travel Network, has elicited from its franchisees, according to Stephanie Abrams, vice president/global marketing for the Englewood Cliffs, N.J.-based travel agency franchisor:
"Matching Miles is magnificent!... We are signing up between seven and 10 new people daily, all of whom are business travelers."
"At last count we had 159 Matching Miles applications. Eighty percent of these are new clients! Some have booked tickets over $1,000; some have booked high-end tours. Some of our new clients are corporations."
"Matching Miles has been a godsend for our agency. Being two years old, we needed a major hook to get the more prestigious accounts away from the more established agencies."
"Our agency opened its doors just this week. Already we have had numerous inquiries from five different states!...At times the phone lines have been so busy we have had difficulty handling all the calls!"
"There is no question, from the quality of the responses our agencies gave us, that the program is working for them -- and dramatically," Abrams says.
Travel Network's trade-marked Matching Miles promotion, inspired by and modeled closely after the airlines' frequent flyer programs, is relatively simple. After filling out an application, agency clients earn Matching Miles certificates toward free air travel every time they book a domestic or international flight on any of eight major domestic airlines. When travelers accumulate at least 25,000 miles in certificates on any particular airline, they may redeem their certificates at the Travel Network agency that processed their applications. Awards, which are transferable, range from one free coach ticket to any gateway destination within the 48 contiguous states (at 25,000 miles) to one free coach ticket to any gateway destination in Asia or the Pacific Rim (120,000 miles).
Matching Miles was designed both to attract new clients to Travel Network's 350-plus franchise locations and to earn the loyalty of existing clients, Abrams explains. "The consumer continually shops. If someone can give them a better deal this week over last week, they'll be shopping for it. I started in this business as a travel agent. I understand the importance of getting that client to come back to you again and again."
Abrams contrasts the program with corporate rebates, emphasizing that Matching Miles allows Travel Network agencies to reward customers who have demonstrated their loyalty. "The awards come as a result of the passenger

spending a great deal of money with the agency. We are by nature anti-rebate. This is more a reward and recognition, because you've already performed -- as opposed to every time you buy a ticket we knock off some money. You show us the productivity, then we're going to reward you, just the way a wholesaler is able to provide a travel agency with an override because you have produced significantly and put enough profit into the company."

Conceived early in the spring of 1994, Matching Miles was launched just after Labor Day last year. Between conception and launch, Abrams put together a comprehensive $500,000 promotional campaign, developing marketing materials to stimulate awareness of the program among business travelers.

The result of her labors was a multifaceted campaign that encompasses store-level promotional tools, support for advertising and publicity at the local level and a national advertising and public relations campaign. "I am a great believer in a saturated-market approach to anything," Abrams says. "You can't do just one thing and rely on that to bring your message home. You need to bombard people with your message."

For the approximately 85% of Travel Network franchisees participating in the Matching Miles program, Travel Network provides a full array of promotional tools, including banners, posters, counter cards, direct mail fliers, ticket stuffers, postcards, fax broadcast forms, buttons for agents to wear, brochure application forms and telemarketing scripts.

Most promotional materials are four-color and printed on high-quality coated stock. Most also feature as their centerpiece a blue and orange globe surrounded by the promotion's slogan: "Fly once... earn twice," which conveys one of the franchisor's central messages about its program -- the fact that, by participating in Travel Network's program, travelers earn double mileage every time they fly, once with the agency and once in their air carrier's frequent flyer plan.

Travel Network also provides advertising and public relations support for franchisees on the local level, preparing Yellow Pages advertising, ad mats and what Abrams calls "Swiss cheese" press releases, into which individual franchisees can insert their agency name.

On the national level, the franchiser launched an advertising campaign in publications read widely by business travelers, notably in-flight magazines, USA Today, and a publication put out by the U.S. Chamber of Commerce.

Consumers who respond to Travel Network's ads are directed to call a central toll-free number, where an automated answering system identifies where callers are dialing from and automatically switches them to their nearest Travel Network franchise.

Key to the success of the Matching Miles promotion, Abrams believes, was Travel Network's public relations campaign supporting it. "I learned a long time ago that you can spend enormous amounts on advertising and promotion and have a wonderful program and product and not much happens. But you get just one sentence in the New York Times and suddenly, like the pet rock, you're an overnight hit.

"When you are doing advertising only, to some degree it's seen as a salesman's pitch. When you get third-party endorsement, it elevates you to a new level -- and it heightens sensitivity to the advertising."

To alert the media to Matching Miles, Travel Network mailed three press releases outlining the program to 620 travel, business and finance editors. Three different cover letters were written, tailored to each of the three target audiences. The agency followed up the mailings with phone calls to the editors.

By any measure, the media campaign was a success. Travel Network's Matching Miles story was picked up by the Associated Press and Reuters wire services and ran in dozens of leading national and international publications, including USA Today, the Los Angeles Times, Consumer Report's

Travel Letter, Time magazine's international edition, the Washington Post, Newsday, the San Francisco Chronicle, the Miami Herald, U.S. News and World Report, Frequent Flyer Magazine and a number of travel trade publications. The media coverage generated a flood of calls to Travel Network agencies, Abrams says. "In an informal sense, I can tell you that in 48 hours following articles in Denver, Atlanta and Tampa papers, they Travel Network agencies| didn't know what to do with themselves. Nobody had enough hands and ears to handle the incoming calls." After an item appeared in Time magazine's international edition in November, Abrams says, "it hit the fan and just kept going. From the earliest stages, we were getting 1,000 calls a week." Abrams says that Travel Network not only has fielded calls from states where it has no offices but from overseas as well.

Abrams suggests there's no mystery to the widespread media coverage of Travel Network's Matching Miles program. "I don't know that we approached the press uniquely," she comments. Rather, she cites the quality of the agency's press releases, the novelty of its program and the impact of

follow-up calls to journalists as instrumental in grabbing the media's attention. "Being first at doing something is always charismatic," she adds.

Asked if there are any potential pitfalls to undertaking a media campaign, Abrams replies that for Travel Network there were none. "We are a solid, forthright, squeaky-clean company. If you are a solid company, then there is no reason why you shouldn't bring your story to the public. If you've got a skeleton in your closet, bringing media attention on yourself may be opening a can of worms."

To date, the only can that Travel Network has opened contained gold, unleashing thousands of new business clients upon franchisees. Now, the agency is hoping to expand the program's reach. Earlier this spring, Travel Network launched its Miles-to-Go promotion, which applies the same frequent traveler reward concept to the leisure market, rewarding clients who purchase cruises, tours and vacations.

The expansion of the program into the leisure market, part of the franchisor's plan from the outset, exemplifies Travel Network's approach to serving its agency owners, Abrams says. "Like all Travel Network programs, the first phase of the Matching Miles program is the first right answer And we never settle for the first right answer. You do something and say that's really good, now we'll re-evaluate, restructure and expand it. Anytime we launch anything, we're always redefining it."

SPECIAL FEATURES: illustration; photograph
COMPANY NAMES: Travel Network Inc.--Achievements and awards
INDUSTRY CODES/NAMES: TRVL Travel and Hospitality
DESCRIPTORS: Travel agents--Achievements and awards; Public relations--Achievements and awards; Sales promotions--Achievements and awards
PRODUCT/INDUSTRY NAMES: 4721000 Travel Agents
SIC CODES: 4724 Travel agencies
FILE SEGMENT: TI File 148

...ABSTRACT: best public relations and promotional campaigns. The agency's Matching Miles promotion, similar to a **frequent flyer program** or **corporate** rebates. Travelers can accumulate **miles** and be awarded in free airline coach tickets. The program is aimed at business travelers...

19950515

8/9,K/15 (Item 3 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

06106565 SUPPLIER NUMBER: 12425503 (THIS IS THE FULL TEXT)
Asiana Airlines launches corporate frequent flyer program. (Brief Article)
Lassiter, Eric
Travel Weekly, v51, n56, p41(1)
July 13, 1992
DOCUMENT TYPE: Brief Article ISSN: 0041-2082 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT
WORD COUNT: 401 LINE COUNT: 00033

TEXT:
LOS ANGELES - Asiana Airlines, a South Korean carrier, has become the third international airline known to offer a **corporate mileage program**, allowing businesses to accumulate and use **frequent flyer** credits in the same manner as individuals.
The Program, called Asiana Corporate Award, allows a corporation to earn mileage to be used for free trips on Asiana.
Corporations with 10 or more traveling employees can enroll in the program at no cost, with travelers earning corporate mileage when they fly Asiana, according to Steve Alexis, the airline's agency sales manager in Los Angeles.
That collective mileage can be redeemed for free travel on Asiana.
Travelers whose corporations are enrolled in the program will continue to earn mileage credits under Asiana's mileage program for individuals, called the Asiana Bonus Club.
The airline began daily B747-400 nonstop service between Los Angeles and Seoul last fall with connecting flights to a number of South Korean and other Asian cities.
The carrier anticipates starting nonstop service to Seoul from San Francisco and New York in December.
The Asiana corporate mileage categories are as follows: 100,000 miles earn two tickets within South Korea; 200,000 miles, a coach ticket to Japan from Seoul; 300,000 miles, one transpacific ticket in coach; 400,000 miles, one transpacific business class ticket, and 500,000 miles earn one transpacific first class ticket.
All free tickets are for roundtrip travel.
Asiana offers 11,904 miles for roundtrip coach travel between Los Angeles and Seoul, with 20% more credit - or 14,285 miles - for business class on that route and 50% more credit - or 17,856 miles - for first class travel.
Based on those figures, it would take 28 Los Angeles-Seoul business class roundtrips to earn one free transpacific business class ticket on that route.
Alexis noted that the corporate mileage can quickly add up when several employees are flying on the airline.
Mileage earned under either Asiana's corporate or individual frequent flyer programs cannot be transferred to other airlines.
The only other U.S. or foreign-flag airlines known to offer corporate mileage programs are Japan Airlines and Lufthansa.
Both airlines started their **corporate frequent flyer** programs years ago.
Asiana's **mileage program** is being administered out of its Los Angeles office.
The carrier pays agents 25% commission for coach tickets and 15% for business and first class tickets.

COMPANY NAMES: Asiana Airlines--Marketing
INDUSTRY CODES/NAMES: TRVL Travel and Hospitality

DESCRIPTORS: Airlines--Marketing; Frequent flyer programs--Marketing
SIC CODES: 4512 Air transportation, scheduled
FILE SEGMENT: TI File 148

TEXT:
...Airlines, a South Korean carrier, has become the third international airline known to offer a **corporate mileage program** , allowing businesses to accumulate and use **frequent flyer** credits in the same manner as individuals.
... known to offer corporate mileage programs are Japan Airlines and Lufthansa.
Both airlines started their **corporate frequent flyer** programs years ago.
Asiana's **mileage program** is being administered out of its Los Angeles office.
The carrier pays agents 25% commission...

19920713

8/9,K/16 (Item 4 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

06046576 SUPPLIER NUMBER: 12528088
Air Miles adds nine corporate **sponsors. (frequent flyer program)**
Aviation Daily, v309, n32, p279(1)
August 14, 1992
ISSN: 0193-4597 LANGUAGE: ENGLISH RECORD TYPE: CITATION

COMPANY NAMES: Adolph Coors Co.--Contracts; Gillette Co.--Contracts; GTE Mobile Communications Inc.--Contracts; Keyes Fibre Co.--Contracts; Lever Brothers Co.--Contracts; Thomas J. Lipton Co.--Contracts; Rexall Co.--Contracts; Scott Paper Co.--Contracts; Van den Bergh Foods Co.--Contracts
INDUSTRY CODES/NAMES: AERO Aerospace and Defense
DESCRIPTORS: Airlines--Services; Frequent flyer programs--Marketing
SIC CODES: 4512 Air transportation, scheduled; 2082 Malt beverages; 3264 Porcelain electrical supplies; 3421 Cutlery; 2844 Toilet preparations; 6719 Holding companies, not elsewhere classified; 2656 Sanitary food containers; 2841 Soap and other detergents; 2034 Dehydrated fruits, vegetables, soups; 2099 Food preparations, not elsewhere classified; 5122 Drugs, proprietaries, and sundries; 2676 Sanitary paper products; 2672 Paper coated and laminated, not elsewhere classified; 2079 Edible fats and oils, not elsewhere classified; 2051 Bread, cake, and related products
FILE SEGMENT: TI File 148

Air Miles adds nine corporate **sponsors. (frequent flyer program)**

19920814

8/9,K/17 (Item 5 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

02820084 SUPPLIER NUMBER: 04191685 (THIS IS THE FULL TEXT)
Frequent flyer programs: who should reap benefits? (Dun's Business Month Focus)
Glab, Jim

Dun's Business Month, v126, p74(2)
April, 1986
ISSN: 0279-3040 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 1604 LINE COUNT: 00124

TEXT:
Frequent Flyer Programs: Who Should Reap Benefits? Everyone who travels on business is very much aware by now that the major airlines give away thousands of free tickets every year to participants in their frequent flyer programs ... plus free hotel stays, rental cars and even cruises. But the travel that earns these bonuses is paid for by corporations, not by the individuals who actually win the awards; as a result, more and more companies are starting to wonder why the free travel benefits shouldn't be reclaimed from employees in order to reduce their overall travel costs.

This can be done, in some cases, although airline policies on the transferability of award coupons differ from one carrier to another. But there's a more important question: Is it a good idea, from an economic and morale standpoint? The answer is not so apparent.

Scrutiny of both sides of this debate leads to these conclusions: (1) Totally unregulated employee participation in frequent flyer programs can actually increase a company's travel costs; (2) Total regulation and appropriation of frequent flyer awards from employees may not be cost-effective; and (3) there is a middle ground that keeps corporate travel costs to a minimum and also permits employees to enjoy free travel.

A totally unregulated company travel policy can lead to increased expenses for a very obvious reason: Many participants in frequent flyer programs will do anything they can to build up their mileage totals to increase the value of their awards. Such corporate travelers tend to become "mileage junkies" and will go out of their way to make as many trips as possible on their favored airline, whatever it costs.

Most corporate travel directors have anecdotes of people who make trips with three stopovers at a much higher air fare than necessary just to stick with their preferred carrier or those who order first class tickets to get extra mileage credits.

The first thing a company must do in determining its own frequent flyer rules is to determine the awards policies at the airlines most likely to be used by traveling employees. If much of the corporate travel is done on routes served by American Airlines, for instance, benefits can be

transfered from the individual who earns them, as long as the transfer is requested in writing.

American, like all other airlines, would prefer that the award go to the person who actually flies the miles, but if the company wants it assigned to someone else for another business trip, "We don't have any way to police that, and we wouldn't try," an American spokesperson says. "It's an employer/employee relationship problem."

Delta Air Lines also permits its frequent flyer awards to be transferred, a company official said, but the recipient must make the request in person at the company's travel agency or a Delta ticket office. At United Airlines, transfer of the awards from one individual to another is permitted as well, an official said.

Perhaps the most flexible approach to the issue is offered by Japan Air Lines, which provides a choice of three frequent flyer programs: a standard "individuals-only" program; the JAL Corporate Passbook, which permits a company to combine the **mileage** of all its travelers into a single account, with the resulting free tickets awarded to the corporation; and JAL Corporate **Mileage** Bank, in which both individuals and their corporate employer can earn free tickets based on **mileage** . Since the programs were introduced about a year ago, some 250 companies have joined

the Passbook plan and more than 100 have signed up for the **Mileage** Bank.
Even if some airlines don't permit their awards coupons to be transferred, it is still possible for a company to make sure that the awards are used to reduce corporate travel expenses. At Texas Instruments in Dallas, for instance, a spokesperson said that those individuals who do the most traveling on business all have their mileage tracked by the corporation's travel agency. When they are found to be approaching the level that can earn a free ticket, the spokesperson said, the employee is called in and asked about his upcoming business travel plans. The employee must use his free ticket for whatever trip costs the most.

"We don't do it for everyone," the spokesperson said; "just for the big travelers." And the resulting benefit to the corporate travel budget is described as "substantial."

According to Thornton Clark, a business travel consultant in Newton, Massachusetts, any corporate effort to reduce travel cost by recapturing frequent flyer benefits "absolutely" depends on a corporation's attitude toward its employees. To work, it requires an extremely tough corporate policy. Almost all the companies that track frequent flyer mileage fail to implement policies tough enough to capture mileage value that's more than the tracking and policing costs," he says.

"The order to turn in your mileage must come from the CEO," Clark says. The policy should also require travelers to belong to the frequent flyer programs that their companies determine and to not only use those airlines, but also the hotels and rental car companies affiliated with those airlines' programs for extra mileage credits. In an effective program, failure to comply means no reimbursement for expenses or even firing.

If all this is done, Clark estimates a company could save about 6% on its total travel budget, not counting meals. However, he cautions that there is one more thing corporate officers must consider: "They must be prepared for violent antagonism and anti-company feeling among key employees--and is that worth it?"

It seems that many corporations are foregoing the opportunity to create an effective frequent traveler policy. To have one at all requires thorough documentation (i.e., tracking) of all company travel, so the company knows who is piling up how many miles on which airlines. A major portion of corporate travel these days is now channeled through large commercial travel agencies such as American Express or Ask Mr. Foster or through consortiums of commercial agencies such as Woodside Management or Associated Travel Nationwide. Virtually all of these travel firms offer mileage tracking programs to corporate clients, but recent industry surveys reveal few takers.

The tracking program "has been a total waste of money," says Patrick O'Shea, president of Associated Travel Nationwide, based in Chicago. "You have the feeling everyone would want it, but they don't." The reason? "It's questionable how much money they can save. A huge amount of travel is required to qualify for a free ticket. If you look at the cost of tracking mileage and the employee relations aspects, you question its worth."

A more important kind of frequent flyer-related tracking ATN offers, O'Shea says, tells the corporation if any employees are not using the lowest air fare or the most direct routing in their company trips. "The key is to get the flagrant abusers," he concludes.

A similar kind of monitoring service is offered by American Express Travel, and it is the key to its recommended corporate, policy for reducing travel costs, while still permitting employees to keep their mileage awards.

"Most companies we talk to feel that as long as it doesn't cost the company any extra money, they don't mind letting the traveler have the bonus," says Judith Dettinger, American Express vice president-consulting services. She suggests adoption of one basic rule: "Require travelers to

buy (a ticket) by price rather than by carrier."
The tracking service, Dettinger says, will provide employers with monthly reports "on which travelers didn't take the lowest air fares, and their reasons. Then they can call him in and say, 'Look, you cost us an extra $4,000 last month,' and make him stop it. It's an approach that works. The travelers are still going to be flying on the major carriers and building up mileage; just not as fast."
One corporate giant that has taken Dettinger's advice is Detroit-based Burroughs Corp.--a company that spends around $100 million a year just on travel, according to Bob Anderson, Burroughs' director of corporate travel. The corporation has consolidated the travel planning of all its offices and plants nationwide through American Express, and makes good use of the ticket price monitoring service, he says.
Basically, Burroughs' policy is that employees must always take "the lowest fare routing that meets our criteria," Anderson explains. "Our criteria are not all that rigorous," he adds--"no more than one intermediate stop, no more than two hours' layover, and so on. The basic objective of our program is to balance the company's need for cost-effectiveness with the traveler's need for consideration." He estimates that Burroughs' annual travel costs have been cut about 20%.
Dettinger and Anderson both note that the key to control of frequent flyer abuse is simple: Don't let the traveler pick the airline himself. Very few companies have taken the choice away from the traveler," Anderson says. "I think if every company had the controls that Burroughs has, the airlines would probably stop the frequent flyer programs," because their key to success--brand loyalty among individual travelers--would no longer be effective.

INDUSTRY CODES/NAMES: BUS Business, General
DESCRIPTORS: Frequent flyer programs--Economic aspects; Business travel--Economic aspects
FILE SEGMENT: MI File 47

... standard "individuals-only" program; the JAL Corporate Passbook, which permits a company to combine the **mileage** of all its travelers into a single account, with the resulting free tickets awarded to the corporation; and JAL Corporate **Mileage** Bank, in which both individuals and their corporate employer can earn free tickets based on **mileage** . Since the programs were introduced about a year ago, some 250 companies have joined the Passbook plan and more than 100 have signed up for the **Mileage** Bank.
Even if some airlines don't permit their awards coupons to be transferred, it...

19860400

8/9,K/18 (Item 1 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

09717901 (THIS IS THE FULLTEXT)
EMPLOYEE PERKS: Best workplaces are revealed
Christine Williamson
PENSIONS & INVESTMENTS, p2
February 07, 2000
JOURNAL CODE: WCPI LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 1172

From midafternoon basketball games to paid sabbaticals, the 13 financial services firms on Fortune's list of the 100 best places to work offer perks rarely seen in other investment management companies.
Among them:
* MFS Investment Management, Boston, sometimes halts afternoon meetings for staff basketball games.
* Charles Schwab & Co., San Francisco, and Frank Russell Co., Tacoma, Wash., give employees paid sabbaticals. Schwab also has a permanent dress code of "business casual" and provides a concierge service for employees.
* American Century Cos. Inc., Kansas City, Mo., offers domestic partner health benefits that let the employee define "family."
Companies ask to be included in the Fortune survey. Two-thirds of a firm's score is based on employee responses to a survey. The other third is based on Fortune's review of the company's materials. Hewitt Associates LLC, Lincolnshire, Ill., helped Fortune design and tabulate the survey.
Other money management-related firms on the list are: Janus Capital Corp., Denver; Northern Trust Corp., Chicago; American Express Financial Corp., Minneapolis; and Goldman, Sachs & Co., New York.
Randall K. Abbott, a senior consultant and practice leader in the Philadelphia office of Watson Wyatt Worldwide, an employee benefits consulting firm, said personalization and fun help companies market themselves as good places to work, in essence creating a brand identity in the employee's mind.
"I would be looking at the people in my organization who manage the most money, if I were a money manager. And I would pick 10 or 20 of them and think about what I could do to tie those people in even more closely, to retain them long term. There will be a different answer for each person, but this personalization, making people happy in the way they want it most, that's what will keep people at the company," Mr. Abbott said.
Here's what a few companies do for their employees:
MFS
MFS Chairman Jeff Shames loves basketball. Company business has been known to cease in the middle of the afternoon, at least for some employees, who head off for pickup games with their boss.
And, when MFS passed the $100 billion mark last year for assets under management, every employee received a $100 bill.
MFS has a gala holiday party, where it gives away trips to extravagant locales, such as 10 days at the Ritz in Hawaii. **Frequent flyer miles** accumulated by the company for **corporate** travel and credit cards fuel the **program** , said Joseph J. Trainor, president of MFS Institutional Advisors Inc.
On extra-snowy Boston days, pizza often is brought in to keep employees happy and warm and, a few times a year, gallons of ice cream and liters of toppings are brought in for ice cream sundae parties. A fall harvest fair in an apple orchard brings families together for apple picking, a barbecue and hay rides and games, said Mr. Trainor.
Schwab
At Schwab, a player in the 401(k) marketplace, management believes that in order to treat customers well, a company needs to treat its employees well, said Beth Sawi, chief administrative officer.
Beginning in April, employees with five years of service will be eligible for four-week paid sabbaticals that can be combined with vacation time. The sabbatical benefit increases to eight weeks after 10 years.
"Our employees work really hard and we want to make sure they get some R&R," she said.
Part of that excellent treatment recently included $100 American Express gift certificates, a way of thanking workers for a successful navigation of the tricky Y2K period, when vacation time was frozen.
Schwab also offers a concierge service that takes care of everything from finding theater tickets for out-of-town relatives to researching home

contractors to helping with solutions to family problems.
"We want to make sure employees have all that they need to eliminate hassles in their lives so they can focus on work," Ms. Sawi said.
Schwab also rewards employees financially, she said. She cited a generous employee stock ownership program that has made 10% of Schwab employees into millionaires, as well as yearly cash performance bonuses, occasional options grants, spot bonuses and a generous 401(k) plan.
"We want employees to be financially tied to Schwab. We want them to know that profits aren't hoarded at the top," Ms. Sawi said.
Schwab also has a commitment to community service and volunteerism, including a big project with Habitat for Humanity. Its peer-nominated Schwab Volunteer of the Year is recognized at the company's annual meeting. The employee's charity of choice receives $5,000 from the company.
Frank Russell
Russell also has a senior exec who heads off on a regular basis to play afternoon basketball, part of a work-life balance program that pervades the whole company, said Craig Ueland, chief operating officer. "People don't want to work just for money. They need to be motivated," he said.
It was Mr. Ueland who inspired Frank Russell to offer a sabbatical program -- eight paid weeks off every 10 years. He was returning to the United States after setting up Russell's Sydney, Australia, office and took a month off without pay to travel with his wife. It turned out to be such a rejuvenating experience that many others at Russell wanted to do the same thing. But Russell officials realized many employees couldn't afford a month without pay, so they instituted the paid sabbatical policy.
Russell folks are no slouches when it comes to community giving. Several Russell employees set up their own charitable foundations with the money they made when Frank Russell was acquired by Northwestern Mutual Life Insurance Co., Milwaukee, in 1998.
The Russell family is also a big benefactor throughout Tacoma, which inspires many employees to contribute both time and money to charity causes, such as Habitat for Humanity and tutoring programs in local schools.
"We have a lot of tree-huggers in the company, outdoors people. It is part of their culture and the culture of the company to literally take care of our people and to take care of the community," Mr. Ueland said.
They take care of their own, too. Russell employees find a flower on their desks on their birthdays and employment anniversaries. And, a big company picnic every year at a local fairground brings families together.
American Century
American Century's founding family, the Stowers, also are benefactors in the company's home town. Employees follow suit: Overall, American Century employees contribute at least 4,500 hours of community service every year.
The company has been known to share the wealth during exceptionally good years. In 1997 and 1999, for example, every employee got an extra paycheck, said spokeswoman Julie Bartels Smith.
American Century also is one of just a few U.S. companies that offers domestic partner medical benefits that allow the employee to designate who -- besides a spouse -- is "family" and should receive medical coverage. The only requirement is that the individual has lived with the employee for at least a year. Some have designated a younger sibling, others an in-law, nanny or significant other.
@@Volume: 28
@@Publication number: 3
@@Word Count: 1162 words

DESCRIPTORS: Company News; Pay Awards & Benefits; Human Resources & Employment
COUNTRY NAMES/CODES: United States of America (US)
REGIONS: Americas; North America; Pacific Rim
SIC CODES/DESCRIPTIONS: 9441 (Administration of Social & Manpower Programs)
NAICS CODES/DESCRIPTIONS: 92313 (Admin of Other Human Resource Programs)

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... gives away trips to extravagant locales, such as 10 days at the Ritz in Hawaii. **Frequent flyer miles** accumulated by the company for **corporate** travel and credit cards fuel the **program** , said Joseph J. Trainor, president of MFS Institutional Advisors Inc.
On extra-snowy Boston days...

20000207
?

will cost under $200 in quantities, plus about $60 for the docking stations that transmit the Folio's stored data to the terminal for authorization. The company also is promoting a new high-speed printer, the Omni 900R, as an accessory at about $225, although other printers are compatible. A restaurant might have several Folios and more than one docking station depending on its size and transaction volume. Restaurant industry observers are taking a cautious look at the new table-top debit terminals. Dennis Lombardi, executive vice president of Technomic Inc., a Chicago-based restaurant industry consulting firm, says the advantages of improved cash flow and cash management are clear pluses for restaurant owners, but he doesn't see many customers wanting to use debit cards in restaurants or using self-service devices in general for credit. "I don't see the customer particularly excited about running their own credit cards through," he says. "A lot of customers want to take a look at the bill and let the waitperson do it." Lombardi also predicts resistance to using debit cards in restaurants in a society in which a credit card can help **accumulate** perks such as **frequent - flyer miles** . "You start getting up to $40 or $50, I think a lot of restaurant (customers) would prefer to defer," he says.

Subscription: $275 per year as of 1/92. Published monthly. Contact Faulkner & Gray, Inc., 118 S. Clinton St., Suite 450, Chicago, IL 60661. Phone (312) 638-0261. FAX (312) 648-9569.

PUBLISHER NAME: Faulkner & Gray, Inc.
INDUSTRY NAMES: BUSN (Any type of business); RETL (Retailing)

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...card for leisure time and family dining. The likelihood that business diners would use a **company credit** card could limit the technology's appeal, Shade admits. "That could be a hindrance," he...

...using debit cards in restaurants in a society in which a credit card can help **accumulate** perks such as **frequent - flyer miles** . "You start getting up to $40 or $50, I think a lot of restaurant (customers...
19940601

5/9,K/3 (Item 1 from file: 16)

07124950 Supplier Number: 59419860 (THIS IS THE FULLTEXT)
EMPLOYEE PERKS: Best workplaces are revealed;MFS, Russell among financial services firms on the list.
Williamson, Christine
Pensions & Investments, v28, p2
Feb 7, 2000
ISSN: 1050-4974
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1161
TEXT:
From midafternoon basketball games to paid sabbaticals, the 13 financial services firms on Fortune's list of the 100 best places to work offer perks rarely seen in other investment management companies.
Among them:
* MFS Investment Management, Boston, sometimes halts afternoon

meetings for staff basketball games.
* Charles Schwab & Co., San Francisco, and Frank Russell Co., Tacoma, Wash., give employees paid sabbaticals. Schwab also has a permanent dress code of "business casual" and provides a concierge service for employees.
* American Century Cos. Inc., Kansas City, Mo., offers domestic partner health benefits that let the employee define "family."
Companies ask to be included in the Fortune survey. Two-thirds of a firm's score is based on employee responses to a survey. The other third is based on Fortune's review of the company's materials. Hewitt Associates LLC, Lincolnshire, Ill., helped Fortune design and tabulate the survey.
Other money management-related firms on the list are: Janus Capital Corp., Denver; Northern Trust Corp., Chicago; American Express Financial Corp., Minneapolis; and Goldman, Sachs & Co., New York.
Randall K. Abbott, a senior consultant and practice leader in the Philadelphia office of Watson Wyatt Worldwide, an employee benefits consulting firm, said personalization and fun help companies market themselves as good places to work, in essence creating a brand identity in the employee's mind.
"I would be looking at the people in my organization who manage the most money, if I were a money manager. And I would pick 10 or 20 of them and think about what I could do to tie those people in even more closely, to retain them long term. There will be a different answer for each person, but this personalization, making people happy in the way they want it most, that's what will keep people at the company," Mr. Abbott said.
Here's what a few companies do for their employees:
MFS
MFS Chairman Jeff Shames loves basketball. Company business has been known to cease in the middle of the afternoon, at least for some employees,

who head off for pickup games with their boss.
And, when MFS passed the $100 billion mark last year for assets under management, every employee received a $100 bill.
MFS has a gala holiday party, where it gives away trips to extravagant locales, such as 10 days at the Ritz in Hawaii. **Frequent flyer miles accumulated** by the **company** for corporate travel and **credit** cards fuel the program, said Joseph J. Trainor, president of MFS Institutional Advisors Inc.
On extra-snowy Boston days, pizza often is brought in to keep employees happy and warm and, a few times a year, gallons of ice cream and liters of toppings are brought in for ice cream sundae parties. A fall harvest fair in an apple orchard brings families together for apple picking, a barbecue and hay rides and games, said Mr. Trainor.
Schwab
At Schwab, a player in the 401(k) marketplace, management believes that in order to treat customers well, a company needs to treat its employees well, said Beth Sawi, chief administrative officer.
Beginning in April, employees with five years of service will be eligible for four-week paid sabbaticals that can be combined with vacation time. The sabbatical benefit increases to eight weeks after 10 years.
"Our employees work really hard and we want to make sure they get some R&R," she said.
Part of that excellent treatment recently included $100 American Express gift certificates, a way of thanking workers for a successful navigation of the tricky Y2K period, when vacation time was frozen.
Schwab also offers a concierge service that takes care of everything from finding theater tickets for out-of-town relatives to researching home contractors to helping with solutions to family problems.
"We want to make sure employees have all that they need to eliminate hassles in their lives so they can focus on work," Ms. Sawi said.
Schwab also rewards employees financially, she said. She cited a

generous employee stock ownership program that has made 10% of Schwab employees into millionaires, as well as yearly cash performance bonuses, occasional options grants, spot bonuses and a generous 401(k) plan.
"We want employees to be financially tied to Schwab. We want them to know that profits aren't hoarded at the top," Ms. Sawi said.
Schwab also has a commitment to community service and volunteerism, including a big project with Habitat for Humanity. Its peer-nominated Schwab Volunteer of the Year is recognized at the company's annual meeting. The employee's charity of choice receives $5,000 from the company.
Frank Russell
Russell also has a senior exec who heads off on a regular basis to play afternoon basketball, part of a work-life balance program that pervades the whole company, said Craig Ueland, chief operating officer.
"People don't want to work just for money. They need to be motivated," he said.
It was Mr. Ueland who inspired Frank Russell to offer a sabbatical program -- eight paid weeks off every 10 years. He was returning to the United States after setting up Russell's Sydney, Australia, office and took a month off without pay to travel with his wife. It turned out to be such a rejuvenating experience that many others at Russell wanted to do the same thing. But Russell officials realized many employees couldn't afford a month without pay, so they instituted the paid sabbatical policy.
Russell folks are no slouches when it comes to community giving. Several Russell employees set up their own charitable foundations with the money they made when Frank Russell was acquired by Northwestern Mutual Life Insurance Co., Milwaukee, in 1998.
The Russell family is also a big benefactor throughout Tacoma, which inspires many employees to contribute both time and money to charity causes, such as Habitat for Humanity and tutoring programs in local schools.
"We have a lot of tree-huggers in the company, outdoors people. It is part of their culture and the culture of the company to literally take care of our people and to take care of the community," Mr. Ueland said.
They take care of their own, too. Russell employees find a flower on their desks on their birthdays and employment anniversaries. And, a big company picnic every year at a local fairground brings families together.
American Century
American Century's founding family, the Stowers, also are benefactors in the company's home town. Employees follow suit: Overall, American Century employees contribute at least 4,500 hours of community service every year.
The company has been known to share the wealth during exceptionally good years. In 1997 and 1999, for example, every employee got an extra paycheck, said spokeswoman Julie Bartels Smith.
American Century also is one of just a few U.S. companies that offers domestic partner medical benefits that allow the employee to designate who -- besides a spouse -- is "family" and should receive medical coverage. The only requirement is that the individual has lived with the employee for at least a year. Some have designated a younger sibling, others an in-law, nanny or significant other.

PUBLISHER NAME: Crain Communications, Inc.
COMPANY NAMES: *Frank Russell Co.; American Century Companies Inc.; Charles Schwab and Company Inc.
EVENT NAMES: *280 (Personnel administration)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *6411000 (Insurance Agents & Brokers); 6211000 (Securities Dealers)
INDUSTRY NAMES: BANK (Banking, Finance and Accounting); BUSN (Any type

of business); INSR (Insurance and Human Resources)
SIC CODES: 6411 (Insurance agents, brokers, & service); 6211 (Security brokers and dealers)
NAICS CODES: 52421 (Insurance Agencies and Brokerages); 52311 (Investment Banking and Securities Dealing)
TICKER SYMBOLS: ACT
SPECIAL FEATURES: LOB; COMPANY

... gives away trips to extravagant locales, such as 10 days at the Ritz in Hawaii. **Frequent flyer miles accumulated** by the **company** for corporate travel and **credit** cards fuel the program, said Joseph J. Trainor, president of MFS Institutional Advisors Inc.
On...
20000207

5/9,K/4 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

11867883 SUPPLIER NUMBER: 59419860 (THIS IS THE FULL TEXT)
EMPLOYEE PERKS: Best workplaces are revealed;MFS, Russell among financial services firms on the list.
Williamson, Christine
Pensions & Investments, 28, 2
Feb 7, 2000
ISSN: 1050-4974 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1226 LINE COUNT: 00099

TEXT:
From midafternoon basketball games to paid sabbaticals, the 13 financial services firms on Fortune's list of the 100 best places to work offer perks rarely seen in other investment management companies.
Among them:
* MFS Investment Management, Boston, sometimes halts afternoon meetings for staff basketball games.
* Charles Schwab & Co., San Francisco, and Frank Russell Co., Tacoma, Wash., give employees paid sabbaticals. Schwab also has a permanent dress code of "business casual" and provides a concierge service for employees.
* American Century Cos. Inc., Kansas City, Mo., offers domestic partner health benefits that let the employee define "family."
Companies ask to be included in the Fortune survey. Two-thirds of a firm's score is based on employee responses to a survey. The other third is based on Fortune's review of the company's materials. Hewitt Associates LLC, Lincolnshire, Ill., helped Fortune design and tabulate the survey.
Other money management-related firms on the list are: Janus Capital Corp., Denver; Northern Trust Corp., Chicago; American Express Financial Corp., Minneapolis; and Goldman, Sachs & Co., New York.
Randall K. Abbott, a senior consultant and practice leader in the Philadelphia office of Watson Wyatt Worldwide, an employee benefits consulting firm, said personalization and fun help companies market themselves as good places to work, in essence creating a brand identity in the employee's mind.
"I would be looking at the people in my organization who manage the most money, if I were a money manager. And I would pick 10 or 20 of them and think about what I could do to tie those people in even more closely, to retain them long term. There will be a different answer for each person, but this personalization, making people happy in the way they want it most, that's what will keep people at the company," Mr. Abbott said.
Here's what a few companies do for their employees:

MFS
MFS Chairman Jeff Shames loves basketball. Company business has been known to cease in the middle of the afternoon, at least for some employees, who head off for pickup games with their boss.
And, when MFS passed the $100 billion mark last year for assets under management, every employee received a $100 bill.
MFS has a gala holiday party, where it gives away trips to extravagant locales, such as 10 days at the Ritz in Hawaii. Frequent flyer miles accumulated by the **company** for corporate travel and **credit** cards fuel the program, said Joseph J. Trainor, president of MFS Institutional Advisors Inc.
On extra-snowy Boston days, pizza often is brought in to keep employees happy and warm and, a few times a year, gallons of ice cream and liters of toppings are brought in for ice cream sundae parties. A fall harvest fair in an apple orchard brings families together for apple picking, a barbecue and hay rides and games, said Mr. Trainor.
Schwab
At Schwab, a player in the 401(k) marketplace, management believes that in order to treat customers well, a company needs to treat its employees well, said Beth Sawi, chief administrative officer.
Beginning in April, employees with five years of service will be eligible for four-week paid sabbaticals that can be combined with vacation time. The sabbatical benefit increases to eight weeks after 10 years.
"Our employees work really hard and we want to make sure they get some R&R," she said.
Part of that excellent treatment recently included $100 American Express gift certificates, a way of thanking workers for a successful

navigation of the tricky Y2K period, when vacation time was frozen.
Schwab also offers a concierge service that takes care of everything from finding theater tickets for out-of-town relatives to researching home contractors to helping with solutions to family problems.
"We want to make sure employees have all that they need to eliminate hassles in their lives so they can focus on work," Ms. Sawi said.
Schwab also rewards employees financially, she said. She cited a generous employee stock ownership program that has made 10% of Schwab employees into millionaires, as well as yearly cash performance bonuses, occasional options grants, spot bonuses and a generous 401(k) plan.
"We want employees to be financially tied to Schwab. We want them to know that profits aren't hoarded at the top," Ms. Sawi said.
Schwab also has a commitment to community service and volunteerism, including a big project with Habitat for Humanity. Its peer-nominated Schwab Volunteer of the Year is recognized at the company's annual meeting. The employee's charity of choice receives $5,000 from the company.
Frank Russell
Russell also has a senior exec who heads off on a regular basis to play afternoon basketball, part of a work-life balance program that pervades the whole company, said Craig Ueland, chief operating officer.
"People don't want to work just for money. They need to be motivated," he said.
It was Mr. Ueland who inspired Frank Russell to offer a sabbatical program -- eight paid weeks off every 10 years. He was returning to the United States after setting up Russell's Sydney, Australia, office and took a month off without pay to travel with his wife. It turned out to be such a rejuvenating experience that many others at Russell wanted to do the same thing. But Russell officials realized many employees couldn't afford a month without pay, so they instituted the paid sabbatical policy.
Russell folks are no slouches when it comes to community giving. Several Russell employees set up their own charitable foundations with the money they made when Frank Russell was acquired by Northwestern

Mutual Life Insurance Co., Milwaukee, in 1998.
The Russell family is also a big benefactor throughout Tacoma, which inspires many employees to contribute both time and money to charity causes, such as Habitat for Humanity and tutoring programs in local schools.
"We have a lot of tree-huggers in the company, outdoors people. It is part of their culture and the culture of the company to literally take care of our people and to take care of the community," Mr. Ueland said.
They take care of their own, too. Russell employees find a flower on their desks on their birthdays and employment anniversaries. And, a big company picnic every year at a local fairground brings families together.
American Century
American Century's founding family, the Stowers, also are benefactors in the company's home town. Employees follow suit: Overall, American Century employees contribute at least 4,500 hours of community service every year.
The company has been known to share the wealth during exceptionally good years. In 1997 and 1999, for example, every employee got an extra paycheck, said spokeswoman Julie Bartels Smith.
American Century also is one of just a few U.S. companies that offers domestic partner medical benefits that allow the employee to designate who -- besides a spouse -- is "family" and should receive medical coverage. The only requirement is that the individual has lived with the employee for at least a year. Some have designated a younger sibling, others an in-law, nanny or significant other.

COMPANY NAMES: Frank Russell Co.--Personnel management; American Century Companies Inc.--Personnel management; Charles Schwab and Company Inc.--Personnel management
INDUSTRY CODES/NAMES: BANK Banking, Finance and Accounting; BUSN Any type of business; INSR Insurance and Human Resources
DESCRIPTORS: Insurance industry--Personnel management; Securities industry--Personnel management
GEOGRAPHIC CODES/NAMES: 1USA United States
PRODUCT/INDUSTRY NAMES: 6411000 (Insurance Agents & Brokers); 6211000 (Securities Dealers)
EVENT CODES/NAMES: 280 Personnel administration
SIC CODES: 6411 Insurance agents, brokers, & service; 6211 Security brokers and dealers
NAICS CODES: 52421 Insurance Agencies and Brokerages; 52311 Investment Banking and Securities Dealing
TICKER SYMBOLS: ACT
FILE SEGMENT: TI File 148

... such as 10 days at the Ritz in Hawaii. Frequent flyer miles accumulated by the **company** for corporate travel and **credit** cards fuel the program, said Joseph J. Trainor, president of MFS Institutional Advisors Inc.
On...

20000207

5/9,K/5 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

10490386 SUPPLIER NUMBER: 21172973 (THIS IS THE FULL TEXT)
"Don't you already have this information?" (business competitiveness

through superior customer service)
Tehrani, Rich
Telemarketing & Call Center Solutions, v17, n3, p12(3)
Sept, 1998
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1925 LINE COUNT: 00140

TEXT:
You don't need extensive market research to realize that the call center market is still in its infancy - All you need is a telephone, a mortgage or a credit card.

America's economy is destined to become a service economy. How many times have we heard this? Service companies are making a killing on Wall Street with huge market capitalization numbers and future business projections are equally impressive.

But for a company to remain competitive, this is only part of the picture Every company needs to have incredible customer service. Insurance, banking, manufacturing ... everyone. So as we approach the next millennium, we have made great strides in customer service and the future looks bright. Right? Wrong!

I recently had two encounters, one with a bank and the other with a credit card company, that were absolutely infuriating. I am not in the banking or credit card business, but I can guarantee you that service is the key to long-term growth in both these industries. Bank advertising seems to be at an all-time high: the airwaves are full of radio and television ads, newspapers are chock full of them and it seems there are billboard ads for them every few miles along our highways. Add to this the fact that electronic banks are popping up everywhere on the Internet and you can conclude that the market seems to be very hot. Couple this with the fact that interest rates are ridiculously low for every bank and you wonder what keeps a customer with their existing bank if another offers a better deal or better service.

Credit card companies constantly send me incentives to get their cards. I have been offered platinum cards, diamond cards, gold cards, free gas, free long-distance, free grocery shopping, free miles, free cash back; credit limits from $20,000 to $100,000, 2.9% interest, 3.9% interest - where does the madness end?

You'd think the largest of the large financial institutions would have this customer service problem licked. They should be models of perfection. They should make sure that under no circumstances would they lose a customer to poor service. These institutions have millions of customers and advertising budgets in the tens of millions of dollars to attract new customers. If they didn't have great customer service, every day a smaller, nimbler competitor would be chasing their prime customers, stealing revenue from their pockets and bread from their tables. This is what I always thought, but boy was I naive.

In the last few months, I have witnessed customer service atrocities that would make me cringe if they came from my company. You wonder if executives in these large financial institutions ever try calling their own customer service lines themselves to see what the average customer has to suffer through.

Case in point is my recent need to acquire a mortgage for a house. After some shopping around, I decided to do business with the company that has also been handling my primary credit card. This is one of the largest banks in the country. When filling out my application and speaking with the representative from the mortgage company I mentioned I had a credit card with the same bank. This had absolutely no effect on cutting down my paperwork. I was a new customer and that was all there was to it - I had no credit history with them, they did not know me from Adam. I was a stranger. My credit card has been with this company for over ten years, yet I wasn't

even in the computer. I mentioned my loyalty but no one cared.
Well, I got the mortgage and all was well for a few months until I realized I needed my credit limit extended on my credit card. So I called the credit card telephone number and told them that I needed my credit limit increased. After a week I received a letter informing me that I would need to send in a copy of my paycheck or a letter from my boss stating how much money I make. I called to tell them that my salary information, in fact my entire life story, was in the mortgage department's computers. I mentioned to the customer service rep that the mortgage department could tell him how many square feet my house has, how many bathrooms, the year it was built; they know my lawyer, they know my accountant, and they even pay my property taxes for me - who knows me better? "I'm sorry sir, it doesn't work like that," I was told politely. "But why not?" I insisted. "Well, you see sir, the mortgage department works on a different computer system than the credit card department and we can't access their information and they can't access our information," he replied, being ever so polite. "Well great, I have their phone number, would you like to call them and double-check the figures I gave you?" I explained, hoping to raffle the agent's feathers a bit. "Mr. Tehrani (now that he used my name I could tell I was getting to him), our corporate policy maintains that the credit limit adjustment department (or some such arcanely named department) must have the document faxed or mailed to us for record-keeping purposes," he said in an agitated tone. I decided I had better things to do at this point than argue on the phone when I knew I was getting nowhere. I figured if "record-keeping purposes" were really that important, they would actually share some of these records with their other internal departments. Who

needs these records? Are the agents getting commission on the number of records they save up? Are the agents archiving records in the computer in competition with each other? A brief flash of squirrel-like agents busily burying nuts in the yard flashed through my head. Well, I lost too much work time on this; I needed to get back to my job.
After a month or so, I forgot all about this encounter. I seem to be on the road more and more these days, and nothing clears my mind and helps me forget my problems like spending hours in an airplane. Thankfully, all my traveling has added up to a wealth of frequent flyer miles.
Frequent flyer miles equate to nobility in airports. I have hundreds of thousands of miles on certain airlines and merely thousands on others. If I fly airline X, I am a traveling god - my mere presence flying standby immediately reduces all other standby passengers in rank. I check in at certain "no wait" lines at airports. Life is good when I fly airline X. Airline Y however, is different. When I fly this airline it seems to be for short hops. I can never accumulate the miles I need to reach the next level of flying status. Once, airline Y made me wait in an airport for 12 hours before I could fly out of the city - I was bumped off 6 standby lists. Recently, when I saw an ad offering a credit card yielding free frequent flyer miles on airline Y, I jumped at the chance. I had visions of reigning as an airport god on this airline as well. Better yet, the **credit** card **company** was the same **company** that offered my secondary **credit** card.
I immediately called the number on the screen and was barraged by questions: Name, age, social security number, etc. I mentioned I already had a card from this company but the agent, although pleasant, seemed unfazed. So I continued for a while until the agent finished the queries and I went back to watching TV.
A few days later, a letter came to my attention telling me that I must submit employment verification. So I found a pay stub and looked for the fax number on the enclosed letter. No fax number? In this day and age? I am impatient - am I supposed to wait another week just for them to get to opening my letter? So I called and asked for the fax number. It turned out

this bank didn't seem to have the same "record keeping" system as the last bank. In this case, only a letter will do. Here we go again. So I patiently explained that I have been a cardmember in good standing for over 12 years. He said, "Oh, Mr. Tehrani, I did not realize this. Please give me your social security number again." Progress, I thought, progress. So I iterated the magic number and, lo and behold, my prior history was revealed to the agent and I no longer needed to submit anything. I hung up satisfied, but my subconscious didn't rest. I thought to myself that if the social security number is a unique identifier, why didn't I get picked up as a long-time customer already. I needed to tell the agent and the company that I am in their computer? This whole situation wasted time, paper, postage and telephone charges. We could have avoided all of this with a simple database query.

Based on these experiences, I know we are still in the nascent stages of a wonderful technology revolution in the call center. These above cases are ridiculous. A small company should be embarrassed, let alone a large company or the hugest of the huge, knowing that this sort of thing takes place in their call centers.

Perhaps you are thinking about your own call center. Do you have these issues brewing? Are your databases in synch? Do they cross-reference and communicate with each other? Do you have call center software designed to catch this sort of problem?

I have issued a challenge. I have picked some of the major companies in the call center industry and presented them with the challenge of solving the above problems. I have asked for the products they would suggest and how they can link together to make sure the above scenarios never happen in your company. Our October issue of C@LL CENTER Solutions(TM) will have a mini-round-up of companies that can tackle this challenge. Please be sure to read it thoroughly so you will ensure your company serves its customers as well as possible.

These types of scenarios remind me of the days when agents used 3 x 5 cards to keep track of their accounts. Call center software vendors have barely scratched the surface - every company needs to make sure its call center data is accessible as needed by all other departments that have outside contact. People are busy and they are getting busier. Every call center must look at the latest products that will be outlined in the next issue and beyond.

To those banks in question: I noticed you subscribe to C@LL CENTER Solutions(TM). It seems to me you may not be reading as carefully as you need to be. Might I suggest that you take these challenges seriously before I or someone else decides to name you in future articles?

SPECIAL FEATURES: illustration; photograph
INDUSTRY CODES/NAMES: ADV Advertising, Marketing and Public Relations; BUSN Any type of business
DESCRIPTORS: Customer service--Management; Telephone answering services--Usage
PRODUCT/INDUSTRY NAMES: 7399510 (Telephone Answering Services)
SIC CODES: 7389 Business services, not elsewhere classified
FILE SEGMENT: TI File 148

... visions of reigning as an airport god on this airline as well.

Better yet, the **credit** card **company** was the same **company** that offered my secondary **credit** card.

I immediately called the number on the screen and was barraged by questions: Name...

19980900

5/9,K/6 (Item 3 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

05444983 SUPPLIER NUMBER: 11270076 (THIS IS THE FULL TEXT)
Executive travel. (special advertising section)
Grondin, James
Financial World, v160, n20, p39(5)
Oct 1, 1991
ISSN: 0015-2064 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 4124 LINE COUNT: 00330

ABSTRACT: Business travel can be both comfortable and economical. Services offered by airlines, railroads, hotels and the rental care industry are analysed along with innovations in telecommunications and business charge cards.

TEXT:
Fuel prices have returned to normal, the economy is starting to pick up, and corporate travel budgets are easing again. Your company has asked its executives to keep T&E expenses reasonable. But that doesn't mean you have to stay at the local motor inn. With the wealth of corporate travel plans and programs available, you can travel in style--and you company can benefit from volume discounts.

Corporations want to find better ways to control the $125 billion or so they expect to spend on business travel and entertainment this year. And employees who travel at company expense want convenience and comfort. It's possible to achieve both, with a little shopping around among some of the deals offered by airlines, hotels, rental car companies and credit/charge cards that service the business traveler.

Most airlines, hotels and rental car companies offer frequent flyer/guest/renter programs that enable you and your company to obtain service upgrades, special amenities and discounts. In addition, most work in partnership with other programs to enable the traveler to receive double bonus points

For example, Hilton Hotels has car rental partners that include Avis and National, and airlines such as American, Delta, United, US Air and Air Canada. So your stay at the Hilton can earn frequent flyer points with any of those airline programs, or bonus points with the car rental companies.

AIRLINES

We become more stringent in the airline industry, generally requiring 14- or 21-day advance booking with fares that are nonrefundable or that carry stiff penalties for cancellation. This makes matters difficult for the business traveler, who is often forced to book and cancel reservations on short notice.

The good new is that USAir recently became the first major airline to relax its rules, cutting 14- and 21-day advance notice requirements down to seven. Furthermore, many nonrefundable fares now carry only a 25% penalty. On fares that formerly required seven-day advance bookings and a 50% penalty, the penalty has been reduced to 10%.

USAir also runs a unique Fearful Flyers Program for aviaphobic passengers (fearful flyers). The seven-week course is conducted on a regular basis and culminates with its graduates flying in a plane, often for the first time in their lives. Thousands of people have taken the course all over the country, and the carrier claims an extraordinary "cure" rate of 97%.

Continental's Y-OnePass program allows members to fly first class for the price of coach. Needless to say, this is a very popular program with business travelers, who often wind up in coach due to last-minute

reservations. "Other airlines have begun similar offerings, but they usually tack on a surcharge. At Continental, there's no extra charge," says David Messing, continental's director of public relations.

Like most major airlines, Continental offers its business and frequent travelers (who are often one and the same) the amenities of a private lounge at most major airport locations. Business travelers can also reserve the President's Club meeting rooms available at many airports.

Cathay Pacific's Marco Polo Club is unlike most frequent flyer programs: Membership is by invitation only for travelers who accrue 22,000 miles within a 6-month period. Privileges include the use of first-class lounges and check-in, baggage and waiting-list priority and special priority reservations.

Cathay Pacific also offers what may be a truly unique service: Give the airline you business card, and it will make the card bilingual, with translations into Chinese, Japanese, Korean or Thai. In addition, the

carrier's Citycheck service allows its passengers to make use of downtown check-in centers in HongKong and avoid lengthy lines at the airport.

Alaska Air has been honored for superior customer service, seating, on-time performance and baggage handling. While the airline has no business class as such, it offers exceptional service in both first class and coach as well as competitive fares and a generous frequent flyer program.

Alaska Air serves the entire West Coast, from Puerto Vallarta, Los Cabos and San Diego to Nome, Juneau, Anchorage and many more--as well as Phoenix, Tucson and, beginning in October, Toronto. The airline is travel partners with TWA, Northwest, SAS and other airlines, as well as car rental companies including National, Budget and Alamo, and hotels such as Hyatt, Weston and others.

Nowadays, international deals are frequent and worldwide travel is common. To meet the needs of corporate globe-trotters, Lufthansa offers International Business Class enhanced service on all of its German, European, and intercontinental flights.

"More than 2,000 companies are enrolled in Lufthansa's Corporate Mileage Dividend Plan," said Lucille Hoshabjian, manager of corporate communications for Lufthansa. "The plan rewards both the company and the employee: Companies earn mileage credit whenever an employee flies, and employees accumulate mileage credits with Lufthansa's **frequent flyer** partners, including United, Delta, USAir and Continental."

Furthermore, Lufthansa offers three "quality guarantees" that could be invaluable for the business traveler who can't afford to miss an important meeting. They guarantee: (1) You will make your connecting flight in Germany, or they'll put you on the next available flight AND give you $200 in compensation; (2) your baggage will arrive with you, or they'll pay $200 over and above any legal claim; and (3) you will have a seat in the class you booked, or you will be upgraded at no extra charge.

Telephone on airplanes are now common, but Singapore Airlines is the first to offer in-flight telephones using satellites. Most air telephone use ground relays, which means you must be over land to place a call. This is a distinct disadvantage for the business traveler flying from Los Angeles to Tokyo with 11 hours over the Pacific. With Singapore Airlines' Skyphone, travelers can call anywhere in the world at any time.

British Airways recently enhanced its program for business travelers, with new first-class airport lounges, quicker check-in, expanded in-flight menus and a revamped executive club. And since time is money too, supersonic flights should not be overlooked by frequent transatlantic travelers. Flying the Concorde on British Airways enables you to arrive in London in time for dinner and a good night's sleep. Or return on the early morning Concorde flight, and arrive in time for a morning meeting in New York. Plus, there's a reduced chance of suffering from jet lag when you fly the Concorde. British Airways' Concorde operates year-around between London

and New York City, Washington, D.C. or Miami.
With an increase in U.S. business relations with South Africa, SAA (South African Airways) offers extraordinary comfort for the business traveler. Gold Class business-class travel enables you to reserve your seat when you book your ticket, while specifying any special dietary or other requirements. There's also a private check-in facility. Aboard your flight, SAA Gold class provides spacious seating and privacy, totally contained from the rest of the plane. SAA's Prestige Club card offers benefits for frequent travelers.
ALL ABOARD!
Amtrak offers a unique alternative to the stresses of air travel for those who want to recharge their batteries and refresh themselves en route to an important business meeting. In addition, traveling by train gives you more time and opportunity to take care of business. There's more leg and seat room, larger tables to spread out your work, and no need to put everything away for take-offs and landings. In addition, Amtrak stations tend to be located in city centers, near downtown business areas.
And train travel may be faster than you think. Metroliner Service between New York City and Washington, D.C., can travel up to 125 mph and make the trip in as little as 2 1/2 hours.
"One of the best-kept secrets in business travel in the Northeast" is the way Clifford Black, director of public affairs for Amtrak, describes Metroliner's Executive Sleeper car. The train leaves Washington in the evening; the Executive Sleeper car is detached in New York while you continue to sleep peacefully until you receive your morning wake-up call, accompanied by a newspaper and continental breakfast. Southbound, you can board the train as early as 9:30 pm--or as late as 3:30 am, if you want to take advantage of night life in the Big Apple.
In September, Amtrak began a prototype conference car on its Metroliner line. You can reserve one of the car's semi-private booths, or use the conference room that seats up to eight for meetings, presentations or rehearsals--complete with VCR, marker board, cellular telephone and conference table.
HOTELS
Nowadays, hotels cater more than ever to the business traveler. Typical services include copying, facsimiles, telex, overnight deliveries, arrangement of secretarial services such as typing and shorthand, and business equipment rental. In addition, many hotels offer translation services, extra telephone, same-day laundry, pressing or dry cleaning, quick video check-out, notary public and in-house work processing. Travelers who use computers may even be able to communicate with their offices from their room via modem.
For business travelers, Marriott Hotels feature guaranteed reservations, express check-out, video check-out, in-room video message retrieval, spacious accommodations that include a separate work area, relaxation center and sleep area. In addition, most Marriotts offer teleconferencing capabilities.
Marriott Honored Guest Awards program for frequent guests is undergoing enhancement. The hotel chain is exploring a new arrival and check-in process, including some testing at certain locations.
Marriott travel patners include Continental, Northwest, TWA, Eastern, US-Air and Hertz. Travelers can accumulate points toward free lodging, vacations and more.
Omni Hotels has shifted its Select Guest program to focus on the frequent traveler during his or her stay, rather than awards that come later. Select Guest members receive preferred treatment during each stay. Also, new programs offer Select Guest Gold members the ability to call as late as 4 pm for same-day reservations. Gold Card membership is available to guests who stay at Omni at least 25 nights annually.
In addition, Omni's "Just for you" privileges--which vary among

locations--include such amenities as the use of health club spas at no extra charge, complimentary faxes and copies, and more. For example, the Omni Berkshire Place in New York City offers complimentary limo service from its midtown location to Wall Street.
Omni's Executive Service Plan kis designed for the needs of the business traveler as well as corporate travel planners. The plan offers corporate discounts based on the volume of rooms booked by the company, and corporate rates that can be negotiated based on travel to certain cities. In addition, Omni's Gavel Service offers help for meeting planners and programs for meetings.
Radisson's Worldwide Hospitality Program is open to companies of all sizes--from Fortune 500 corporations to small businesses. The program features guaranteed rates at all properties, special corporate account numbers with a toll-free reservation phone line, and the ability to consolidate total volume to earn greater discounts. The average corporate discount is 5% to 10%, but it can increase to 20% depending on company usage. Under the plan, Radisson does all the work, including keeping track of company usage. Radisson publishes its rates in an annual directory and guarantees them for the entire year.
The clientele served by Nikko Hotels is international, with a heavy business orientation. The hotels are distinguished by their serene Japanese decor and service. Business traveler services include Nikko Executive Touch, or N.E.X.T. The plan offers special rates and additional services to executive of corporations that use Nikko Hotels frequently.
N.E.X.T offers benefits for corporations that include special rates on suites, guaranteed preffered room rates, preffered availability, direct billing upon request and periodic productivity reports. For the individual traveler, the benefits include preregistration of rooms, complimentary use of Health Clubs, express check-in and check-out, early check-in and late check-out and free transportation to business districts in select cities (currently available in New York, san Francisco and Atlanta).
Westin hotels & Resorts offers the Premier Guest Program, which now includes the use of preregistration for some members to speed check-in. Also, members fill out personal preference profiles--such as smoking versus non-smoking room, desired room location, etc.--that enable Westin to help match the room to the traveler's needs. Upon arrival, Premier members pick up a preregistration packet--that includes their room key--and go directly to the preassigned room, without stopping to sign a credit card receipt or registration card. And Westin Executive Club floors offer additional privacy, service and upgraded amenities. Many clubs have their own private entrances and includes an Executive Club lounge.
Inter-Continental's guest recognition program is called the Six Continents Club, and 90% of its members are business travelers. The Club, which recently celebrated its 25th anniversary, was the first hotel program of its kind. For even more frequent guests, the Executive Card is available

for those who stay 30 or more nights within a 12-month period. Executive Card members receive express check-in, early check-in, a guaranteed room with 72-hour advance reservation and complimentary upgrades to suites or executive floors, which are currently available in San Francisco, New Orleans and Chicago.
At the Sheraton Grande in downtown Los Angeles, each room has its own private butler service. Your butler brings complimentary coffe or tea service with your morning wake-up call, along with newspaper delivery, ice delivery, complimentary pressing, laundry pickup and return, delivery of faxes and special messages and provision of incidentals. The Sheraton Grande also offers an innovative package that's designed for attorneys who stay for long jury trials in the nearby court district. "The trial package" offers war rooms, limo service to and from the courthouse, two phone lines in each room, and more.

Sheraton is currently involved in a massive program to upgrade standards for its business guests. As part of the program, the hotel chain is investing more than $1 billion to upgrade its properties, especially its flagship hotels in business centers such as New York and Los Angeles.
Hilton's Honors guest reward program has a three-tier structure, depending on the number of hotel stays. In addition, Hilton recently introduced "Point Stretcher" awards, which enable guests to save up to 50% on the points normally required for free hotel stays.
Four Seasons Hotels offer 24-hour room service, which can be critical to the global traveler whose jet-lagged stomach may say it's breakfast time at 2 am.
The hotels also feature one-hour pressing service, overnight dry cleaning, complimentary shoe shine and complete business facilities. The Four Seasons Executive Suite offers 50% larger rooms at a price that's only 15% higher.
The Four Seasons is currently opening a new hotel in Tokyo, which will be its first in Asia. Set around Japanese gardens, the hotel rooms will be the largest in Tokyo. To serve the omnipresent Japanese business traveler, many Four Seasons hotels in North America and London offer special Asian services such as Japanese breakfasts and robes, brochures printed in Japanese and employees who speak Japanese.
RENTAL CARS
The car rental market is an $8.7 billion-a-year-enterprise, and a large chunk of that is spent by the corporate traveler.
Avis tries harder with its Preffered Express service at over 30 major U.S. airports: "No counters, no paperwork, no stopping, no hasles," says Avis public relations manager Ray Noble. "For the traveler in a hurry, it's an ideal way to run directly from the plane to a waiting car. Your rental agreement is already on the seat with your car keys. Preffered Express is part of our Preffered Rental program for frequent renters."
Avis has numerous travel partners, including hotels such as Hilton, Hyatt, Sheraton, Best Western and Stouffers; and airlines Air Canada, American, Delta, Qantas, Midwest Express/Skyway, and Pan Am, among others.
Alamo has a new Express Return feature--a high-speed, computer-based car return system that uses hand-held terminals and portable printers to complete rental agreements and print receipts within seconds after a vehicle pulls in. This service is available at many high-volume business travel locations, such as Los Angeles, Boston, Chicago, ATlanta and Washington, D.C.'s National Airport. Alamo guarantees curbside delivery of an indestructible receipt in 60 seconds or less after the car pulls up. Indestructible receipt? Well, yes, almost: it's waterproof, smudgeproof and therefore, travelproof, so it's still intact when you get back to the office.
Alamo also has a unique "Waiver Savers" plan that is the first three-tiered collision damage waiver program. Unlike other plans, it's not "all or nothing" to get CDW coverage. Alamo offers three levels of coverage that can be tailored to virtually every renter's needs, and the prices are inexpensive: $3, $6 and $9 (most CDW coverage costs $11 to $13).
At 30 major airport locations, Hertz offers the ultimate in "no-hassle" car renting: no stopping, no signing and no searching--your name appears on an electronic sign on your car. And, get this: You don't even have to start the engine. When the bus drops you off at your car, the engine is on, the trunk is open and the heater or AC is on.
Hertz-1 Club membership is free and enables quick rentals because all customer data is kept on computer. Hertz rental counters also offer computerized driving directions and video maps of routes, so travelers in unfamiliar cities can find hotels, corporate and government facilities, conventional halls, sports arenas, nearby cities and towns, and even local AM/FM radio station listings.
Hertz also offers instant return and express return service,

self-service return (Just slip your Club card in an ATM-style machine), and some locations have in-car mobile phones that are activated by credit card. Many Hertz airport locations even have their own flight monitors that show flight arrival and departure times and gate assignments at your courtesy bus stop.

TELECOMMUNICATIONS

For the international traveler who may only speak English, AT&T USADirect service lets you connect with English-speaking U.S. operators in 95 countries around the world. You have the option of billing the call to an AT&T calling card or as a collect call. In about 75% of the countries where it's available, you can dial direct using any telephone.

"By using AT&T USADirect Service, travelers avoid paying extra local taxes and minimize their hotel subcharges, which are generally higher than AT&T international calling rates," says Frank Sunder, product marketing manager for AT&T USADirect Service." You can make continuous number of calls by just hitting the 'pound' sign [#] in between each call--so you only pay the hotel for one call."

As an example, Sunder notes that a 10-minute direct-dial call from a hotel in Rome to the U.S. costs about $55. The same call is less than $14 with a USADirect Service call charged to an AT&T calling card Savings typically range from 20% to 75% off hotel direct-dial rates, according to Sunder.

For international travelers, AT&T also offers a handy wallet card that lists telephone access codes for every country. You can call 1-800-874-4000 to get a free wallet card and receive information 24 hours a day about AT&T USADirect Service.

AT&T's "Green Pages" contain an impressive preay of international information for the business traveler. The book, which fits in a briefcase, gives the lowdown on local weather, what not to say, important telephone numbers for embassies, hotels, airlines, restaurants, and more. You can also find out whether business relationships in the country you're visiting are formal or informal.

Also, AT&T Language Line Service offer 24-hour telephone access to translators who will translate virtually any language or dialect into English. For $3.50 a minute plus international toll charges, you can talk to an interpreter and bill the call to a credit card. Callers can also access Language Line Service toll-free in the U.S.

BUSINESS CHARGE CARDS

Travel and Entertainment is the third-largest controllable expense for most companies, following salaries and data processing. Yet many companies don't exert proper control over T&E expenses through the use of corporate charge/credit cards.

American Express Travel Management Services launched the Small Business Services program, which provides travel management and programs such as automatic accident disability insurance, an auto fleet leasing program, discounted rates on company car leases, reduced hotel rates, quarterly management reports, car rental loss and damage insurance and a purchasing plan for office equipment.

For larger companies, the American Express Corporate Card offers travel insurance, guaranteed hotel reservations, worldwide emergency assistance, business travelers accident insurance, baggage insurance and a global assist hotline. And you can use the card to get cash at 29,000 ATMs worldwide.

Employees are issued cash advances and are billed on their corporate card, while the company is reimbursed for the advance by American Express. Billing options include: Central Billing (consolidated by airline charges, car rental charges and all fees and bills by card user), Individual Billing (for each card user), and Individual Billing, Central Payment (bills are paid centrally, while card users reconcile their expenses individually).

In other respects, the Corporate Card functions just like the

individual American Express card: No pre-set spending limit, signed receipts with each month's bill, and American Express trademarks such as the Buyer's Assurance Protection Plan and Purchase Protection Plan to replace lost, stolen or damaged goods.
The Air Travel Card, started by a few U.S. airlines in 1936, is the only charge card exclusively for air travel. Today the card is issued by some 28 domestic and international airlines and is accepted by over 200 airlines as well as Amtrak.
The Air Travel Card will help corporate travel managers to control travel expenses and develop a customized billing plan to make reconciliation easy. The card also offers an unlimited credit line with no annual fee or other charges, and automatic flight insurance program of $200,000, with optional plans for increased coverage.
Each card is coded with restrictions to prevent its misuse. Charges are fully documented, travel-only charges that virtually eliminate card abuse. You can even choose the option of a cardless account so company travel is verified through a central account number on file with your travel agency.
The Air Travel Card also lets you select the type of customized billing statements from the airline of your choice to best suit your company's accounting system and management needs. The card provides customized billing from airlines for easier reconciliation, spending analysis by airline and help in separating fully deductible business travel from partially deductible expenses.

Use of the Visa Business Card is promoted by five of the U.S. top eight travel agencies, and more than half of the top 20--quite an achievement, especially since competitor American Express owns one of the top eight agencies. Visa boasts acceptance at more than nine million locations worldwide--more than any other card. A relatively new entrant to the business card market, Visa increased the number of its business cardholders by more than 50% from April 1991 to July 1991.
The Visa Gold and Visa Business cards provide emergency assistance 24 hours a day, pre-trip assistance, auto rental loss damage insurance, worldwide cash access at 330,000 Visa member offices and at 62,000 ATMs in 39 countries through the Visa ATM Network, emergency cash and guaranteed check cashing, travel accident insurance, purchase security and extended protection for purchase made with the card.

SPECIAL FEATURES: illustration; photograph
INDUSTRY CODES/NAMES: BANK Banking, Finance and Accounting
DESCRIPTORS: Business travel--Services
FILE SEGMENT: MI File 47

... earn mileage credit whenever an employee flies, and employees accumulate mileage credits with Lufthansa's **frequent flyer** partners, including United, Delta, USAir and Continental."
Furthermore, Lufthansa offers three "quality guarantees" that could
...

19911001

5/9,K/7 (Item 1 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

09717901 (THIS IS THE FULLTEXT)
EMPLOYEE PERKS: Best workplaces are revealed

Christine Williamson
PENSIONS & INVESTMENTS, p2
February 07, 2000
JOURNAL CODE: WCPI LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 1172

From midafternoon basketball games to paid sabbaticals, the 13 financial services firms on Fortune's list of the 100 best places to work offer perks rarely seen in other investment management companies.
Among them:
* MFS Investment Management, Boston, sometimes halts afternoon meetings for staff basketball games.
* Charles Schwab & Co., San Francisco, and Frank Russell Co., Tacoma, Wash., give employees paid sabbaticals. Schwab also has a permanent dress code of "business casual" and provides a concierge service for employees.
* American Century Cos. Inc., Kansas City, Mo., offers domestic partner health benefits that let the employee define "family."
Companies ask to be included in the Fortune survey. Two-thirds of a firm's score is based on employee responses to a survey. The other third is based on Fortune's review of the company's materials. Hewitt Associates LLC, Lincolnshire, Ill., helped Fortune design and tabulate the survey.
Other money management-related firms on the list are: Janus Capital Corp., Denver; Northern Trust Corp., Chicago; American Express Financial Corp., Minneapolis; and Goldman, Sachs & Co., New York.
Randall K. Abbott, a senior consultant and practice leader in the Philadelphia office of Watson Wyatt Worldwide, an employee benefits consulting firm, said personalization and fun help companies market themselves as good places to work, in essence creating a brand identity in the employee's mind.
"I would be looking at the people in my organization who manage the most money, if I were a money manager. And I would pick 10 or 20 of them and think about what I could do to tie those people in even more closely, to retain them long term. There will be a different answer for each person, but this personalization, making people happy in the way they want it most, that's what will keep people at the company," Mr. Abbott said.
Here's what a few companies do for their employees:
MFS
MFS Chairman Jeff Shames loves basketball. Company business has been known to cease in the middle of the afternoon, at least for some employees, who head off for pickup games with their boss.
And, when MFS passed the $100 billion mark last year for assets under management, every employee received a $100 bill.
MFS has a gala holiday party, where it gives away trips to extravagant locales, such as 10 days at the Ritz in Hawaii. Frequent flyer miles accumulated by the **company** for corporate travel and **credit** cards fuel the program, said Joseph J. Trainor, president of MFS Institutional Advisors Inc.
On extra-snowy Boston days, pizza often is brought in to keep employees happy and warm and, a few times a year, gallons of ice cream and liters of toppings are brought in for ice cream sundae parties. A fall harvest fair in an apple orchard brings families together for apple picking, a barbecue and hay rides and games, said Mr. Trainor.
Schwab
At Schwab, a player in the 401(k) marketplace, management believes that in order to treat customers well, a company needs to treat its employees well, said Beth Sawi, chief administrative officer.
Beginning in April, employees with five years of service will be eligible for four-week paid sabbaticals that can be combined with vacation time. The sabbatical benefit increases to eight weeks after 10 years.
"Our employees work really hard and we want to make sure they get some

R&R," she said.
Part of that excellent treatment recently included $100 American Express gift certificates, a way of thanking workers for a successful navigation of the tricky Y2K period, when vacation time was frozen.
Schwab also offers a concierge service that takes care of everything from finding theater tickets for out-of-town relatives to researching home contractors to helping with solutions to family problems.
"We want to make sure employees have all that they need to eliminate hassles in their lives so they can focus on work," Ms. Sawi said.
Schwab also rewards employees financially, she said. She cited a generous employee stock ownership program that has made 10% of Schwab employees into millionaires, as well as yearly cash performance bonuses, occasional options grants, spot bonuses and a generous 401(k) plan.
"We want employees to be financially tied to Schwab. We want them to know that profits aren't hoarded at the top," Ms. Sawi said.
Schwab also has a commitment to community service and volunteerism, including a big project with Habitat for Humanity. Its peer-nominated Schwab Volunteer of the Year is recognized at the company's annual meeting. The employee's charity of choice receives $5,000 from the company.
Frank Russell
Russell also has a senior exec who heads off on a regular basis to play afternoon basketball, part of a work-life balance program that pervades the whole company, said Craig Ueland, chief operating officer.
"People don't want to work just for money. They need to be motivated," he said.
It was Mr. Ueland who inspired Frank Russell to offer a sabbatical program -- eight paid weeks off every 10 years. He was returning to the United States after setting up Russell's Sydney, Australia, office and took a month off without pay to travel with his wife. It turned out to be such a rejuvenating experience that many others at Russell wanted to do the same thing. But Russell officials realized many employees couldn't afford a month without pay, so they instituted the paid sabbatical policy.
Russell folks are no slouches when it comes to community giving. Several Russell employees set up their own charitable foundations with the money they made when Frank Russell was acquired by Northwestern Mutual Life Insurance Co., Milwaukee, in 1998.
The Russell family is also a big benefactor throughout Tacoma, which inspires many employees to contribute both time and money to charity causes, such as Habitat for Humanity and tutoring programs in local schools.
"We have a lot of tree-huggers in the company, outdoors people. It is part of their culture and the culture of the company to literally take care of our people and to take care of the community," Mr. Ueland said.
They take care of their own, too. Russell employees find a flower on their desks on their birthdays and employment anniversaries. And, a big company picnic every year at a local fairground brings families together.
American Century
American Century's founding family, the Stowers, also are benefactors in the company's home town. Employees follow suit: Overall, American Century employees contribute at least 4,500 hours of community service every year.
The company has been known to share the wealth during exceptionally good years. In 1997 and 1999, for example, every employee got an extra paycheck, said spokeswoman Julie Bartels Smith.
American Century also is one of just a few U.S. companies that offers domestic partner medical benefits that allow the employee to designate who -- besides a spouse -- is "family" and should receive medical coverage. The only requirement is that the individual has lived with the employee for at least a year. Some have designated a younger sibling, others an in-law, nanny or significant other.

@@Volume: 28
@@Publication number: 3
@@Word Count: 1162 words

DESCRIPTORS: Company News; Pay Awards & Benefits; Human Resources & Employment
COUNTRY NAMES/CODES: United States of America (US)
REGIONS: Americas; North America; Pacific Rim
SIC CODES/DESCRIPTIONS: 9441 (Administration of Social & Manpower Programs)
NAICS CODES/DESCRIPTIONS: 92313 (Admin of Other Human Resource Programs)

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... such as 10 days at the Ritz in Hawaii. Frequent flyer miles accumulated by the **company** for corporate travel and **credit** cards fuel the program, said Joseph J. Trainor, president of MFS Institutional Advisors Inc.
On...

20000207

5/9,K/8 (Item 1 from file: 583)
DIALOG(R)File 583:Gale Group Globalbase(TM)

09298294
Asiana forms marketing alliance with BC Card
SOUTH KOREA: ASIANA, BC CARD JOIN HANDS
The Korea Herald (XBF) 24 May 2000 p.8

Language: ENGLISH

South Korea's Asiana Airlines and BC Card, the country's largest **credit** card **company** , have agreed to jointly launch the "BC Asiana Club Card" in June 2000. The card is a combination of credit card and **frequent flyer** scheme and it allows cardholders to earn free round-trip tickets according to **accumulated mileage** . Asiana intends to offer one mile per Won 1,000 in one-time or instalment payment.

COMPANY: BC CARD; ASIANA AIRLINES

PRODUCT: Credit Card Services (6020CC); Nonbank Credit Card Firms (6141); Passenger Air Transport (4501); Scheduled Airlines (4510);
EVENT: Company Formation (14);
COUNTRY: South Korea (9SOK);

South Korea's Asiana Airlines and BC Card, the country's largest **credit** card **company** , have agreed to jointly launch the "BC Asiana Club Card" in June 2000. The card is a combination of credit card and **frequent flyer** scheme and it allows cardholders to earn free round-trip tickets according to **accumulated mileage** . Asiana intends to offer one mile per Won 1,000 in one-time or instalment...

2000

5/9,K/9 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01150452
An internet payment and loading system using a smart card
Internetsystem zum Zahlen und Laden mit einer Chipkarte
Systeme de paiement et de rechargement par Internet, utilisant une carte a **puce**
PATENT ASSIGNEE:
VISA INTERNATIONAL SERVICE ASSOCIATION, (560813), 900 Metro Center Boulevard, Foster City, CA 94404, (US), (Applicant designated States: all)
INVENTOR:
Davis, Virgil M., 1121 Runnymead Drive, Los Altos, CA 94024, (US)
Cutino, Suzanne C., 431 Arkansas Street, San Francisco, CA 94107, (US)
Berg, Michael J., 2644 Belmont Canyon Rd, Belmont, CA 94002, (US)
Conklin, Fredrick Sidney, 26 Alida Court, Oakland, CA 94602, (US)
Pringle, Steven John, 5174 Miles Avenue, Oakland, CA 94618, (US)
LEGAL REPRESENTATIVE:
Finnie, Peter John et al (79521), Gill Jennings & Every, Broadgate House, 7 Eldon Street, London EC2M 7LH, (GB)
PATENT (CC, No, Kind, Date): EP 1003139 A2 000524 (Basic)
EP 1003139 A3 011017
APPLICATION (CC, No, Date): EP 2000200558 980430;
PRIORITY (CC, No, Date): US 45883 P 970430; US 951614 971016
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
RELATED PARENT NUMBER(S) - PN (AN):
EP 1023705 (EP 98920079)
INTERNATIONAL PATENT CLASS (V7): G07F-019/00; G07F-007/08; G06F-017/60

ABSTRACT EP 1003139 A2
An architecture and system loads and uses a smart card (5) for payment of goods and/or services purchased on-line over the Internet (202). A client module on a client terminal (204) controls the interaction with a consumer and interfaces to a card reader (210) which accepts the consumer's smart card (5) and allows loading and debiting of the card. Debiting works in conjunction with a merchant server (208) and a payment server (206). Loading works in conjunction with a bank server (860) and a load server (862). The Internet provides the routing functionality between the client terminal and the various servers. A payment server (206) on the Internet includes a computer and a security module (or a security card (218) in a terminal (214)) to handle the transaction, data store and collection. A merchant server (208) advertises the goods and/or services offered by a merchant for sale on a web site. The merchant contracts with an acquirer to accept smart card payments for goods and/or services purchased over the Internet. A consumer uses his smart card (5) at the client terminal (204) in order to purchase goods and/or services from the remote merchant server (208). The client terminal sends a draw request to the payment server. The payment server processes, confirms and replies to the merchant server (optionally by way of the client terminal). To load value, the client terminal (204) requests a load from a user account at the bank server (860). A load request is sent from the card (5) to the load server (862) which processes, confirms and replies to the bank server (optionally by way of the client terminal). The bank transfers loaded funds to the card issuer (108) for later settlement for a merchant from whom the user purchases goods with value on the card.

ABSTRACT WORD COUNT: 301
NOTE:
Figure number on first page: 17

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 000524 A2 Published application without search report
Change: 001227 A2 Legal representative(s) changed 20001109
Search Report: 011017 A3 Separate publication of the search report
Examination: 020619 A2 Date of request for examination: 20020412
Change: 020703 A2 Legal representative(s) changed 20020517
Change: 020703 A2 Legal representative(s) changed 20020517
Examination: 050316 A2 Date of dispatch of the first examination report: 20050201
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count
CLAIMS A (English) 200021 1549
SPEC A (English) 200021 19201
Total word count - document A 20750
Total word count - document B 0
Total word count - documents A + B 20750

SPECIFICATION

Field of the Invention

The present invention relates generally to a payment system and a value loading system using a computer network. More specifically, the present invention relates to a payment system and a value loading system for a smart card using an open network such as the Internet.

Background to the Invention

With the explosive growth in open networks (such as the Internet) over the past several years and the rapid increase in the number of consumers with access to the World Wide Web, there has been a great deal of interest in the development of electronic commerce on the Internet. Traditional financial transactions are being transformed.

A variety of service providers have introduced payment schemes to support the purchase of goods or services on-line in a virtual merchant environment. These approaches have used several models based on traditional payment methods existing in the face-to-face retail market, including credit/debit cards, checks and cash. However, for a variety of reasons, various of these numerous schemes have particular drawbacks.

Currently, a consumer may use his or her traditional credit or debit card to make a purchase over the Internet. A consumer simply supplies his card account number which is then transmitted across the Internet to a merchant and the payment transaction is completed in the traditional manner for a credit card. Often, these account numbers are transmitted over the Internet with extremely limited or no security. Security can be improved through use of the "Secure Electronic Transaction" protocol published by Visa International and Mastercard in 1996. These transactions still require some form of card validation and performance of a balance check. These checks are performed on-line between the merchant, an acquirer and an issuing bank, a process which can become time consuming and inefficient when the value of the transaction is low, or when a number of small value transactions will be taking place in a short time span.

The electronic check is modeled on the paper check, but is initiated electronically using digital signature and public cryptography. Deposits are gathered by banks via electronic mail and cleared through existing channels such as the Automated Clearing House (ACH). However, use of such

an electronic check by a consumer has various drawbacks. For one, digital signatures and public encryption necessitate use of a certifying authority adding additional entities and "net" trips to the transaction. Also, cardholder registration is needed.
Other Internet payment alternatives are modeled on cash transactions and include a variety of schemes. With CyberCash, the consumer appends his credit card number to an electronic invoice received from the merchant, returns the credit card number to the merchant which is then processed and forwarded on to CyberCash where it is then treated like a normal credit card transaction. However, this technique suffers from some of the disadvantages discussed above with respect to traditional credit card transaction on the Internet and requires additional work by the merchant in processing the credit card number. Debit transactions may also be completed but require a consumer to open a CyberCash account in advance.
A digital, token-based system for Internet transactions has been implemented by DigiCash. With DigiCash, so-called "digital coins" are purchased from DigiCash from a prefunded deposit account and stored on the consumer's hard drive. These digital coins are then used for an Internet transaction with a merchant. This scheme has disadvantages in that the consumer must first set up a relationship with DigiCash and use a credit card or similar instrument to purchase these digital coins, which then must be downloaded to the consumer's computer. This transaction can be time consuming for the consumer and is subject to fraud. In addition, a merchant must be set up to not only accept these digital coins, but also to verify their authenticity, to confirm the transaction, and then finally to forward these numbers on to his bank in order to finally get paid. One drawback from the merchant's point of view is that much of the transaction work must be performed by the merchant.
Another scheme for completing an Internet transaction is offered by First Virtual Holding, Inc. First Virtual offers a software solution based upon a unique identification number and electronic mail confirmation. To use this scheme, a consumer opens a special account with First Virtual and then receives a confidential identification number.

When the consumer wishes to purchase a product or service over the Internet, he or she sends an electronic mail message containing the confidential identification number to the merchant. The merchant then sends the number to First Virtual by electronic mail for verification and identification of the customer. First Virtual then confirms with the consumer by electronic mail that the consumer did indeed initiate the transaction and wishes to make the purchase. There are drawbacks to this scheme in that the consumer must first open a special account with First Virtual. Also, the merchant must communicate with First Virtual to identify the customer and to identify the customer's credit card account number that is identified by the confidential identification number.
Aside from payment schemes over the Internet, a technique in use for performing a financial transaction at a stand-alone terminal uses a smart card. A smart card is typically a credit card-sized plastic card that includes a semiconductor chip for holding the digital equivalent of cash directly, instead of pointing to an account or providing credits. When a card of this kind is used to make a purchase, the digital equivalent of cash is transferred to the merchant's "cash register" and then to a financial institution. Stored-value cards are either replenishable (value can be reloaded onto the card using a terminal) or non-replenishable (the card is decremented in value for each transaction and thrown away when all its value is gone).
Physically, a smart card often resembles a traditional "credit" card having one or more semiconductor devices attached to a module embedded in the card, providing contacts to the outside world. The card can interface

with a point-of-sale terminal, an ATM, or a card reader integrated into a telephone, a computer, a vending machine, or any other appliance. A microcontroller semiconductor device embedded in "processor" smart card allows the card to undertake a range of computational operations, protected storage, encryption and decision making. Such a microcontroller typically includes a microprocessor, memory, and other functional hardware elements. Various types of cards are described in "The Advanced Card Report: Smart Card Primer", Kenneth R. Ayer and Joseph F. Schuler, The Schuler Consultancy, 1993, which is hereby incorporated by reference.

One example of a smart card implemented as a processor card is illustrated in FIG. 1. Of course, a smart card may be implemented in many ways, and need not necessarily include a microprocessor or other features. The smart card may be programmed with various types of functionality, such as a stored-value application; credit/debit; loyalty programs, etc. For the purpose of this disclosure, card 5 is programmed at least with a stored-value application, and will be referred to as "stored-value" card 5.

Stored-value card 5 has an embedded microcontroller 10 that includes a microprocessor 12, random access memory (RAM) 14, read-only memory (ROM) 16, non-volatile memory 18, an encryption module 22, and a card reader interface 24. Other features of the microcontroller may be present but are not shown, such as a clock, a random number generator, interrupt control, control logic, a charge pump, power connections, and interface contacts that allow the card to communicate with the outside world. Microprocessor 12 is any suitable central processing unit for executing commands and controlling the device. RAM 14 serves as storage for calculated results and as stack memory. ROM 16 stores the operating system, fixed data, standard routines, and look up tables. Non-volatile memory 18 (such as EPROM or EEPROM) serves to store information that must not be lost when the card is disconnected from a power source but that must also be alterable to accommodate data specific to individual cards or any changes possible over the card lifetime. This information might include a card identification number, a personal identification number, authorization levels, cash balances, credit limits, etc. Encryption module 22 is an optional hardware module used for performing a variety of encryption algorithms. Card reader interface 24 includes the software and hardware necessary for communication with the outside world. A wide variety of interfaces are possible. By way of example, interface 24 may provide a contact interface, a close-coupled interface, a remote-coupled interface, or a variety of other interfaces. With a contact interface, signals from the microcontroller are routed to a number of metal contacts on the outside of the card which come in physical contact with similar contacts of a card reader device.

One possible use of a stored-value card by a consumer is illustrated in FIG. 2. FIG. 2 illustrates a block diagram of a customer operated service payment terminal 50. A customer typically uses such a service payment terminal in a face-to-face environment in order to purchase goods in a store or directly from the terminal itself. Service payment terminal 50 can be an attended device or it can be integrated into a self-service device such as a vending machine or public telephone. For example, the service payment terminal may be incorporated into a soda machine in order to dispense sodas to a customer in which the customer pays by inserting the stored-value card. Or, the service payment terminal may be a point-of-sale terminal such as is found at a checkout counter where a customer inserts his stored-value card in order to purchase goods. Service payment terminal 50 includes a router 51, a user interface 52, a card handler/reader 54, a security card handler 56, a security card 58, a terminal application 60, a data store 64 and a concentration point handler 66. Router 51 is hardware and software for routing information

between functional blocks. User interface 52 controls the status of displays on the terminal and supplies instructions to the user. For example, the user interface provides instructions relating to insertion of stored-value card 5 or security card 58. Also, the user interface provides instructions and/or buttons for the customer to interact with terminal application 60 in order to purchase goods and/or services. Card handler 54 provides a physical card reader and associated software for accepting and communicating with stored-value card 5. Similarly, security card handler 56 provides a card reader and associated software for communicating with security card 58. In conjunction with security card handler 56, security card 58 controls the command sequence of the terminal and provides transaction and a batch security.

Terminal application 60 receives commands and information about the transaction and initiates the actual purchase. In addition, terminal application 60 is responsible for all application specific functionality such as guiding the customer through the use of the terminal via a display, and for providing all hardware and software needed to provide the user with a good and/or service once it has been informed by the security card that an appropriate value has been deducted from the stored-value card.

Data store 64 controls the storage of purchase transactions and totals. Concentration point handler 66 controls the sending and receiving of information to and from a concentration point. Concentration point 68 is a staging computer that communicates with any number of service payment terminals to collect batches of transactions. The concentration point then sends these transaction batches to a clearing and administration system for processing (such as in FIG. 3). Once processed, batch acknowledgments, along with other system updates are sent to the terminals via the concentration point. The concentration point ensures a successful transfer of data between service payment terminals and the clearing and administration system, and prevents overloading of the clearing and administration system. The service provider contracts with a concentration point for collection of the service payments. The concentration point may also be an existing central facility such as a telephone company that collects its own payments from card telephones. Such a service payment terminal 50 allows a customer to use a stored-value card for the payment of goods and/or services, generates a payment result from a transaction, and bundles individual payment results into a collection for transfer to a clearing and administration system, which then transfers funds that had been debited from a customer's stored-value card to the merchant whose goods and/or services had been purchased from the terminal.

FIG. 3 illustrates an environment 100 useful for issuing stored-value cards and reconciling transactions performed with such a card. A terminal supplier 102 builds the equipment used by a service provider 104 to provide goods and/or services to customers having a stored-value card at a service payment terminal 50. Card Supplier 106 contracts with an integrated circuit manufacturer and a card manufacturer for integrated circuits and plastic card bodies, then embeds the integrated circuits into the cards and initializes them with a serial number. It then delivers the cards to card issuer 108. In conjunction with clearing and administration system 110 (such as a system provided by Visa International of Foster City, CA), card issuer 108 personalizes new cards and then transfers these cards to individuals (cardholders 112). The cardholder may then charge the card with value prior to use. Alternatively, the card may come with value already loaded. The cardholder 112 may then use the card at a service payment terminal 50 to purchase goods and/or services from service provider 104. Terminal 50 then debits the value from the card, thus creating a service payment.

Periodically, all transactions are sent in a data file from terminal 50 via concentration point 68 and an acquirer 114 to clearing and batch administration system 110 along with accumulated service payment batches from other terminals. Based upon this collection data, clearing and administration system 110 then receives money from card issuer 108 which had originally come from cardholder 112. Clearing and administration system 110 then transfers a lump sum to acquirer 114 using a suitable settlement service (such as one provided by Visa International) to pay the various service providers having a relationship with acquirer 114. Based upon the previous collection data, acquirer 114 then transfers an appropriate amount of money to each service provider 104 reflecting the value of the goods and/or services that that service provider had provided that day to cardholders based upon deductions from their stored-value cards.

Although such a service payment terminal described above is useful for the on-site purchase of goods by a consumer with a smart card, it does not permit the purchase of goods and/or services by a customer over a network. Nor does such a terminal permit the immediate transfer of electronic information to a consumer's computer. Service payment terminals are typically specially-designed units of hardware and software located at a merchant site. Furthermore, the service payment terminal is designed to integrate into one hardware location the functions of the terminal application (providing goods and/or services), a card handler for the stored-value card, and the transaction management embodied in the security card. Such a design is not suitable for transactions where a customer may wish to perform a transaction from almost any location (including the home or office) quickly and easily with a minimum of prearranged set-up and expense. Furthermore, although various Internet payment schemes have been suggested, they are not oriented toward small value transactions, and do not allow the use of a smart card for transactions over the Internet.

Thus, it would be desirable to have an architecture and system that would allow a consumer to quickly and easily perform transactions over an open network such as the Internet using a smart card. It is also desirable to have an architecture and system in which a user may use a smart card for both purchases over the Internet as well as purchases at existing service payment terminals.

However, in order to purchase, the card must be loaded with value first. Value can be loaded onto a stored-value card in a variety of ways. Currently, it is inconvenient for a user to load value onto his or her stored-value card. A user must physically travel to a bank or other institution that has an automated teller machine (ATM) or other similar device in order to load value on to his or her stored-value card. The user can insert money into the machine and have a corresponding value put onto the stored-value card, the user can use a debit card to deduct value from the user's account at the bank for transfer to the card, or a credit card can be used as the source of funds to be transferred to the stored-value card. In either case, the user must travel to the bank to load value. Further creating difficulty is that not all banks or other financial institutions have such a machine for loading value onto a user's stored-value card.

Accordingly, it would also be desirable to have a technique to allow a user to conveniently and easily load value onto a stored-value card.

Summary of the Invention

To achieve the foregoing, and in accordance with the purposes of the present invention, an architecture and system is disclosed that enables the use of a smart card for payment of goods and/or services purchased on-line over an open network such as the Internet. Further, an architecture and system is disclosed that enables a smart card to be

loaded with value on-line over an open network such as the Internet.
In a first aspect, the present invention provides an electronic commerce payment solution offering consumers an on-line equivalent to purchases with cash or coins. It extends the notion of a smart card to the Internet marketplace, providing an alternative for low-value transactions. The present invention facilitates not only the purchase of physical goods, but also the purchase of digital merchandise (such as electronic information).
In one embodiment of the present invention, a client server on a client terminal controls the interactionwith the consumer and interfaces to a card reader which accepts the consumer's smart card, which, in one specific embodiment, includes a stored-value application. For the purposes of this description, the smart card with a stored-value application used in embodiments of the invention will be simply referred to as a "stored-value card." A payment server on the Internet includes a computer and terminals that contain security cards to handle the transaction, data store and collection. Also connected to the client terminal and the payment server over the Internet is a merchant server advertising the goods and/or services offered by a merchant for sale. In one embodiment of the invention, the merchant server includes a web site and the merchant has contracted with an acquirer to accept stored-value card payments for goods and/or services purchased over the Internet. Thus, a consumer may use his or her stored-value card at a client terminal location in order to purchase goods and/or services from a remote merchant server. The Internet provides the routing functionality among the client terminal, merchant server and payment server.
From the consumer's perspective, the present invention operates in a similar fashion as using a stored-value card in a real merchant environment. The transaction process is similar to the interaction between a stored-value card and a service payment terminal in a face-to-face merchant environment, but with functionality distributed across the Internet between the card reading device located where the customer is, the merchant server advertising the merchant's wares, and a payment server with a security card that manages the transaction. All of these entities may be physically remote from one another with router functionality being provided by the Internet. The present invention is easy to use. A consumer need not establish a new relationship with a bank or other Internet service company, nor create a special Internet deposit account in order to begin purchasing goods and/or services on the Internet. A consumer simply makes use of currently available stored-value cards in order to make an Internet purchase.
When browsing merchant store fronts on the Internet and deciding to purchase goods and/or services, the cardholder selects the stored-value card payment option offered by the merchant. The cardholder then inserts his or her card into a card reader attached to a personal computer (for example). The cardholder's balance and purchase amount are displayed, the cardholder approves the purchase, and the amount is deducted from the value stored on the stored-value card. The transaction amount is captured by the security card or the merchant server for subsequent batch settlement through a clearing and administration system to the issuer and acquirer. In one embodiment, the transaction security and authentication for the system follows a similar methodology as that used in an actual service payment terminal between a stored-value card and the security card in the terminal. Advantageously, a customer may make use of pre-existing stored-value cards for purchases over the Internet without any prior arrangement of an account, purchases of credits or tokens, or establishment of a new relationship with a bank or other company.
In addition, once a value has been deducted from the stored-value card, the merchant has been informed, and the security card in the payment server has recorded the transaction, an existing clearing and

administration system may be used to reconcile the transaction and to pay the appropriate parties. Advantageously, a new system and methodology for reconciling transactions need not be developed or implemented. A pre-existing clearing and administration system may be used which greatly simplifies implementation of the present invention.

Use of a stored-value card as payment for Internet transactions provides numerous advantages. For example, a stored-value card can be used in small transactions where credit cards or checks would be unrealistic. Other advantages to the consumer include enhancing the value of a stored-value card by enabling access to both real and Internet merchant environments with a single card. The present invention also allows an anonymous payment solution for transactions over open networks. Furthermore, in one embodiment of the invention the stored-value card is implemented on a traditional credit card; a single card thus provides payment solutions for both low and high value transactions.

In addition, use of a stored-value card is extremely advantageous for small dollar amount transactions. Often, consumers are reluctant to use, and merchants are reluctant to accept, credit card transactions for small dollar amounts. For the consumer and the merchant dealing with many of these small transactions can be a bookkeeping headache and may not be worth the expense. A merchant may also be unlikely to accept a credit card for a small dollar amount transaction because of the service fees per transaction. By permitting the use of a stored-value card to make purchases over the Internet for small dollar amounts, a merchant may very well be able to begin charging for goods and/or services that he had been

providing for free in the past. One embodiment of the invention works well with purchases of under $10.00, although purchases of any amount may be made.

The present invention also provides numerous advantages to merchants who wish to sell goods and/or services over the Internet. For example, the present invention provides a payment solution for low-value transactions, enabling merchants to offer a wider range of digital merchandise. A merchant is also provided a method to recover costs of services not previously charged for, and is provided immediate access to an existing, and rapidly growing, cardholder base. Furthermore, the present invention integrates into an existing clearing and administration system meaning that the merchant need not implement or become familiar with new procedures for reconciliation of transactions.

Furthermore, a merchant need only make a minimal investment in time and money to take advantage of the present invention and to accept payments over the Internet. The merchant need not engage in the development of complex software or accounting procedures. Thus, smaller merchants will especially benefit from the present invention. By establishing a business relationship with an acquirer and incorporating standard merchant software, a merchant is ready to begin selling goods and/or services from his web site. Because a smart card with a stored-value application is used, the payment server and the client terminal perform the details of the transaction and a merchant is relieved from having to control and keep track of a transaction. Also, the payment server and its associated security cards manage and provide security for the transaction. From a merchant's point of view, the merchant knows that a consumer desires to purchase an item and that a cost has been transmitted to the consumer, thus, when the merchant receives a confirmation message, the merchant may release the item to the consumer. The merchant need not be concerned about security nor be responsible for authenticating a stored-value card nor for determining a balance on the card. Of course, a payment server could coexist along with the merchant server or could even be the same computer. That is, a merchant could implement payment server functionality at its own site if it so desired.

In a second aspect of the present invention, a loading technique allows the consumer to conveniently load value on to his or her stored-value card from any suitable device via an open network such as the Internet. A consumer is allowed to use any suitable computer at the home, office or elsewhere in order to connect to his bank or other financial institution. Using appropriate message integrity, value is transferred from the bank to the consumer's stored-value card. At the same time, the corresponding value is transferred from the bank to the stored-value card issuer through existing networks for later settlement with a merchant from whom the consumer purchases goods or services. Advantageously, this embodiment makes use of an existing clearing and administration system for eventual settlement of the transaction between the merchant and the card issuer. Also, the transaction is fully auditable and a log of previous transactions is stored on the card for later display. Thus, a consumer may conveniently load value on to his or her card while a high level of security is maintained and the card issuer can take advantage of unspent funds on the card.

From the consumer's perspective, the present invention operates in a fashion similar to loading a stored-value card at an ATM machine, except that the consumer need not insert cash or an additional debit or credit card, nor need travel to a bank. The loading functionality is distributed across the Internet between the card reading device located where the customer is, a bank server holding the consumer's account, and a load server with a host security module that provides security. All of these entities may be physically remote from one another with router functionality being provided by the Internet.

Furthermore, a bank need only make a minimal investment in time and money to take advantage of the present invention in order to allow its customers to load value from their existing accounts over the Internet. The bank need not engage in the development of complex custom software or accounting procedures. By incorporating software libraries, a bank is ready to begin loading value onto its customer's cards from its web site. Preferably, libraries are provided that interface with an existing server at a bank to facilitate the building of an HTML page. Because a smart card with a stored-value application is used, the bank server, load server and client terminal perform the details of the transaction and the bank itself is relieved from having to control and keep track of a transaction. Also, the load server and stored-value card manage and provide security for the transaction. I.e., the bank need not be concerned about security nor be responsible for authenticating a stored-value card nor for determining a balance on the card. Of course, a load server could coexist alongside the bank server or could even be the same computer. That is, a bank could implement load server functionality at its own site if it so desired. In a preferred embodiment, the load server and its security module is provided by a separate financial institution or by a third-party processor.

Both of the payment and loading aspects of the present invention provide benefits to issuers and acquirers. Expansion of the functionality for a stored-value card increases revenue opportunities from cardholders and merchants. Also, there may be new merchant marketing opportunities for acquirers. The present invention also offers a micro-payment solution for electronic commerce without the need to introduce a separate product or brand or to establish new service provider relationships. In addition, in one specific embodiment of the invention, funds that are loaded onto a card are transferred from the loading bank to the card issuer so that the issuer may take advantage of the funds on the card until they are spent. A further advantage of both aspects of the present invention is its ability to minimize transaction traffic on the Internet and to minimize the amount of time that a security card (or a security module) is tied up with one transaction. In the payment aspect, by emulating security card

commands issued to a stored-value card, a client terminal is able to receive and group responses for transmission to a payment server all at once, rather than one-by-one over the Internet. The payment server is then able to emulate a stored-value card as it interacts with the security card in delivering the responses to the security card. The result is less message traffic over the Internet, saving time and interrupts.

Also, by delivering an expected stored-value card signature to the payment server, the security card is relieved from having to compare the signatures itself, and may release sooner and move on to a new transaction. The payment server may also deliver the expected stored-value card signature to the client terminal or merchant server for comparison, thus reducing to one round trip the message traffic between the payment server and the client terminal.

The present invention is suitable for use with any type of stored-value card that is able to store an amount and to decrement a value upon a command. In one embodiment of the invention, a stored-value card implemented as a processor card works well. Use of a processor card has advantages where information processing is done on the card rather than in the terminal or host computer. Processor cards allow encryption to be done by the card, allow generation of signatures, and can accommodate multiple passwords or personal identification (such as biometrics that uniquely identify the holder of the card). Processor cards also provide increased data security, an anti-fraud capability, flexibility in applications, a multi-purpose capability, and off-line validation. Because high telecommunication costs and/or low reliability of a network may make on-line authorization impractical, a stored-value card with the capability for performing off-line processing and authentication by itself is extremely valuable.

Brief Description of the Drawings

Examples of the present invention will now be described in detail with reference to the accompanying drawings, in which:

FIG. 1 is a block diagram of an example of a stored-value card useful in embodiments of the present invention;

FIG. 2 is a block diagram of a service payment terminal in which a stored-value card may be inserted to purchase merchandise;

FIG. 3 is a block diagram of an example of a clearing and administration system useful for reconciling financial transactions received from a service payment terminal;

FIG. 4 illustrates an architecture and system for payment over the Internet using a stored-value card.

FIG. 5 illustrates a payment embodiment of the present invention;

FIG. 6 illustrates another payment embodiment of the present invention in which the security card releases earlier;

FIG. 7 illustrates yet another payment embodiment of the present invention having fewer round trip messages between the client terminal and payment server;

FIG. 8 illustrates still another payment embodiment of the present invention in which the merchant server compares stored-value card signatures;

FIG. 9 illustrates an added encryption layer useful for embodiments of the present invention;

FIG. 10 is a flowchart describing a user's perspective of a stored-value card purchase transaction using the present invention;

FIGS. 11A-11D are a flowchart describing the processing of a user purchase using an embodiment of the present invention;

FIG. 12 is a flowchart describing the alternative embodiment of FIG. 6;

FIG. 13 is a flowchart describing the alternative embodiment of FIG.

7;
FIG. 14 is a flowchart describing the alternative embodiment of FIG. 8;
FIGS. 15A and 15B are a flowchart describing the added security layer of FIG. 9;
FIG. 16 illustrates an architecture and system for authentication over an internet using a stored-value card;
FIG. 17 illustrates a system for loading value onto a stored-value card according to one embodiment of the present invention;
FIGS. 18A-18D are a flowchart describing the loading of a consumer's stored-value card using an embodiment of the present invention; and,
FIG. 19 is a block diagram of a typical computer system suitable for use in embodiments of the present invention.

Detailed Description

The present invention separates the functionality involved in a transaction using a stored-value card in order to take advantage of the routing capabilities of the Internet. FIG. 4 illustrates symbolically an architecture 200 for an internet payment system involving a smart card, such as a smart card having a stored-value capability. An internet loading system is shown in FIG. 17 and may have similar functionality as described below. Shown is an internet 202, a client terminal 204, a payment server 206 and a merchant server 208. Local cardholder functions including a consumer card interface, display and accept/cancel options are performed at client terminal 204. Payment functions including security card control, data store and use of a concentration point are performed by payment server 206. The presentation and eventual delivery of goods and/or services by a merchant are performed under control of merchant server 208. The internet 202 performs routing functions between each entity. It should be appreciated that internet 202 may take the form of the Internet currently in use, or may also be any other open network implemented using any combination of computer, telephone, microwave, satellite, and/or cable networks.

Basically, client terminal 204 controls the interaction with a user and interfaces to card reader 210 which accepts a smart card having a stored-value application. For simplicity, throughout the remainder of this specification, card 5 will be referred to as a stored-value card (SVC) 5. Payment server 206 communicates directly with a terminal or through a concentrator 212 that handles any number of terminals 214-216 each having a security card 218 and 220 respectively. Payment server 206 also communicates with concentration point 68 for transmission of transaction data to a clearing and administration system. Database 223 stores all suitable information passing through payment server 206 for each transaction. Use of such a database allows any number of merchants (or merchant servers) to use payment server 206 for transactions. Payment server 206 controls payment functions such as handling the attached terminals, managing data base 223 and collection functions. Merchant server 208 is a site that has contracted with an acquirer to accept stored-value card transactions as payments for goods and/or services purchased over the Internet.

Stored-value card 5 may take a variety of forms and is useful in many situations where it is desirable to store monetary value on a card that a consumer may use. In general, a stored-value card is any card or similar device that is able to store a value that is decremented when the card is used. The card may be purchased complete with a stored-value or value may be later added to the card by a user. Such cards may also have their value replenished. Of course, a stored-value card need not be in the form of the traditional credit card, but could appear in any form and of any material that is able to store value and be manipulated by a user for a payment transaction. By way of example, other forms that a stored-value

card may take are any electronic representations. Further, the functionality of stored-value card 5 may be implemented in software on client terminal 204, that is, card 5 may be a "virtual" card.

A stored-value card may also perform a variety of functions in addition to simply storing value. A card may be dedicated to the storing value or may contain memory and programs for other applications as well. By way of example, an "electronic wallet" refers to a processor card that can execute a variety of financial transactions and identification functions. Such a card may serve debit, credit, prepayment, and other functions. A stored-value card typically includes information such as a bank identifier number, a sequence number, a purchase key, a load key, an update key, an expiration date, a transaction counter, a session key, etc., in addition to a running balance.

A stored-value card may also be termed a prepayment card, a cash card, or a decrement-in-value card. A stored-value card may also be implemented by using a variety of card technologies. By way of example, a stored-value card is typically implemented as a card containing one or more integrated circuits. One example of an integrated circuit card is a memory card that has a semiconductor device for storing information but lacks calculating capability. Another example of an integrated circuit card is a processor card that has not only memory but also a microcontroller to enable the card to make decision. A processor card may also be termed a microprocessor card or a "smart card".

A processor card may include an encryption module in order to provide a variety of security precautions. By way of example, security precautions may include simple PIN numbers, biometrics, simple algorithms, or sophisticated algorithms such as the Data Encryption Standard (DES) or Rivest, Shamir, Adelman (RSA) encryption. The card is thus able to use these precautions to verify users, card readers, etc., to validate security cards and/or to provide a unique signature. Preferably card 5 includes any number of keys known to the card issuer that are used during the course of a payment or load transaction to generate signatures for validation of the stored-value card, validation of the security card or module, and validation of the system itself.

Client terminal 204 is any suitable device for interacting with a stored-valued card 5 and for communicating over a network to a payment server or a merchant server. By way of example, client terminal 204 may be a mainframe computer, a work station, a personal computer, a kiosk, or any type of service payment terminal that a consumer might use to purchase goods and/or services. Furthermore, client terminal 204 may also be embodied in any portable device such as a laptop computer, a cellular telephone, or any variety of a personal digital assistant (PDA) such as those made by Apple Computer, Inc. or by U.S. Robotics. Card reader 210 is any suitable interface device that functions to transfer information and commands between client terminal 204 and stored-value card 5. By way of example, card reader 210 may be a card reader manufactured by Fischer-Farr International of Naples, Florida, by Hewlett-Packard of Palo Alto, California, by Schlumberger, by Gem Plus, etc. Card reader 210 may take any variety of forms such as a stand alone unit, integrated with the client terminal, attached to the keyboard of the client terminal, or even built in to a floppy disk-sized unit capable of being read from a disk drive of the client terminal, etc.

Client terminal 204 includes client code module 224 and card reader module 226. Reader module 226 may be implemented using any suitable software and libraries for communicating with card reader 210 and its actual implementation will depend upon the type of card reader used. Client module 224 controls communication between the client terminal, the card reader, the payment server and the merchant server. Client module 224 may be implemented using any suitable code. In one embodiment of the invention, client module 224 is implemented using a combination of "C"

code and a Java applet. The applet is also supplemented with parameters from an HTML page sent from the merchant server. It is contemplated that Java code works well for implementing the modules on the client, payment and merchant servers because it is platform independent, and could even replace the "C" and "C++" code used.

Client module 224 is also responsible for controlling displays to the user and for the interaction between the card and the card reader. The module also builds the draw request message after receiving all of the start-up information from the card and the amount of the purchase from the merchant server. The client module is able to communicate with all components on the Internet, either directly or indirectly.

Payment server 206 includes payment code module 228 and terminal interface 230. As with client terminal 204, payment server 206 may be implemented using any suitable computer. By way of example, a personal computer works well. There may be one payment server for each merchant server or a single payment server may service any number of merchant servers. Alternatively, there may be multiple payment servers for a single merchant. In addition, payment server 206 need not be remote from merchant server 208 but may be located at the same site and have a different Internet address, or the payment server and the merchant server may even be implemented on the same computer. Payment server 206 is designed to facilitate the communication between the user's stored-value card and a terminal's security card. If a part of a transaction fails to complete, the payment server may notify the participating system components.

Payment module 228 may be implemented using any suitable code. By way of example, payment module 228 is implemented using a combination of "C" code, "C++" code and Java code. Payment module 228 is, in one specific embodiment, a multi-threaded process that can service multiple concurrent

client applet transactions on demand. The module is responsible for controlling all interactions with the terminals and their concentrator including the transaction collection function. For individual transactions, the payment module controls the message flows and logs interim results. When an applet connects with the payment server, it creates a transaction thread to support the transaction through its life cycle. Each thread, in turn, assigns a terminal for communication. Having a one-to-one correspondence between transaction threads and terminals has been found to provide desirable results.

Terminal interface 230 is any suitable set of software and libraries for communicating with a terminal 214 either directly or, as shown, through terminal concentrator 212. The actual implementation of terminal interface 230 will depend upon the type of terminal used. A terminal such as 214 may be any suitable terminal such as are known in the art. By way of example, an iq Delta 2010 terminal made by Schlumberger has been found to provide desirable results. Such a terminal may support a variety of commands originating from the terminal interface. These commands emulate the normal responses that an attached terminal would pass from the stored-value card to the security card. The actual security card commands are held in the terminal while the terminal performs the tasks necessary to simulate the presence of a stored-value card.

Security card 218 may be any suitable security card such as are known in the art (often referred to as a Purchase Secure Application Module--PSAM). In other embodiments, the functionality of security card 218 can be replaced by a hardware security module, could be implemented in hardware within the payment server, or could even be implemented in software.

By way of example, security card 218 is a removable credit card-sized processor card that is programmed to process and store data relating to financial transactions. Security card 218 contains a microchip embedded

in the card that enables the security card to authenticate and to validate the user's stored-value card. If a user stored-value card is accepted by the security card, and the stored-value card contains sufficient value, the security card guarantees that the merchant providing the goods and/or services receives payment according to the amount deducted from the stored-value card for the goods and/or services rendered. In a preferred embodiment, the security card also contains DES purchase security keys and authenticates the stored-value card during a purchase transaction and secures the payment and collection totals. A security card also stores signature algorithms for stored-value cards in use. A security card may also contain a transaction identifier for the current transaction, a financial sum of all transactions remaining to be settled, a session key, and master keys for all stored-value cards in use. Further, the security card may contain generations of keys, blocked card indicators, date of last update, multiple card programs, different currency rates and additional security.

Concentration point 68 is a staging computer that communicates with terminals to collect batches of purchase transactions. The concentration point then sends these transaction batches to a clearing and administration system for processing. Once processed, batch acknowledgments, along with other system updates, are sent back to the terminals via the concentration point.

Merchant server 208 includes a merchant code module 232. Merchant server 208 may be implemented upon any suitable computer capable of communicating with and presenting information to users over an internet. Merchant code module 232 may be implemented using any suitable code. By way of example, merchant module 232 may be implemented using a combination of Perl, HTML, and Java code. Merchant server 208 is typically a generic web server customized for the merchant's business. Merchant server 208 may include databases, CGI scripts and back-office programs that produce HTML pages for an Internet user.

A brief discussion of the flow of a transaction now follows. During a financial transaction, the client terminal and merchant server exchange information 234 via internet 202. Each transaction initiated by a user has a transaction identifier created at the merchant server, and a merchant identifier unique to the payment server is also available from the merchant server. Client module 224 and the payment server also use this unique transaction identifier for tracking and logging information about the transaction. Merchant server 208 generates a unique identification of the transaction, completes other required parameters, encrypts as appropriate, and builds an HTML page and sends it to the client terminal. The client module interacts 235 with the stored-value card and builds a draw request message containing related card information, the purchase amount, and other information supplied by the merchant server.

The client terminal then communicates 236 with payment server 206, first by forwarding the draw request to the payment server. Payment server 206 verifies the transaction to determine if it is a valid transaction from a known merchant. The transaction is logged into the payment server's transaction database 223. Upon completion of a transaction, payment server 206 builds a result message containing the identification of the transaction and signs it. The message is then routed to merchant server 208 via client terminal 204. Merchant server 208 then validates the result message. After determining that the transaction was successful, merchant server 208 creates an HTML page for the purchased information and sends it to client terminal 204. Alternatively, the merchant may also deliver purchased goods to the user at this point. It is also possible for the payment server and the merchant server to communicate information 238 directly between themselves. Preferably, as client terminal 204 has already established

communication with the merchant server and the payment server, links 234 and 236 are used to exchange information between the payment server and the merchant server, rather than establishing a new link 238.
FIG. 10 is a flowchart describing an embodiment of the present invention from a user's perspective such as may occur with the embodiment of the invention shown in FIG. 4. In step 502, a user acquires and adds value to a stored-value card. Alternatively, a user may acquire a stored-value card that already contains value. This stored-value card may take the form of any of the above-described stored-value cards that are able to store value and to debit value from the card. In step 504 the user accesses the merchant server web site via communication link 234 over the Internet. This access of a web site may be performed in any suitable fashion such as by using any commercially available web browser. In step 506 the user inserts a stored-value card in card reader 210 at the user's terminal. Alternatively, the user may insert the card before accessing the web site, or even after the selection of goods and/or services from the merchant web site. In step 508 the user browses the merchant web site and selects goods and/or services for purchase from the merchant using the web site interface that the merchant has provided. The user then selects an appropriate button on the merchant web site to indicate what the user wishes to purchase. Next, in step 510 the user receives a total sale amount from the merchant server and is directed to actuate a button on the web site indicating that the user wishes to proceed with the purchase using the stored-value card.
In step 512 the architecture and system of the present invention (such as is shown in FIG. 4, for example) processes the user order by way of the payment server, terminal and security card. In step 514, the user's stored-value card is debited by the total sale amount and the user receives a "debited" message at the user's terminal. This message is optional if the system is designed so as to not inform the user of this debit. In step 516 the user receives a confirmation message from the merchant server indicating that the transaction has been completed. The user may now download the purchased information and/or receive a receipt for goods and/or services to be rendered or delivered from the merchant at a later date. In step 518 the merchant, via a clearing and administration system, receives payment to its bank account for the goods and/or services rendered by way of information collected from the payment server. In one embodiment of the invention, an existing clearing and administration system is used, as well as an existing methodology for transferring information from a security card for later reconciliation. This use of an existing "back end" allows systems of the invention to be implemented quickly and cheaply. This approach also ensures that cards used in the system are compatible with other stored-value terminals.
FIG. 5 illustrates a detailed embodiment of internet payment architecture 200 having client terminal 204, payment server 206 and merchant server 208. A stored-value card 5 is in communication with client terminal 204, and a security card 218 inside a terminal 214 is in communication with payment server 206. Not shown for simplicity in this figure are other elements of the system shown in FIG. 4. One embodiment of a technique by which a financial transaction may be completed over the Internet will now be described using the flowchart of FIGS. 11A through 11D with reference to FIG. 5.
It should be appreciated that a wide variety of terminology may be used to describe message flow throughout the architecture. For example, the terminology used herein to describe the sequential messages draw request, debit, success, and confirmation, may also be referred to by the respective terminology: draw request, debit IEP, debit response, and debit result (or message result).

Initially, a suitable web browser of client terminal 204 is used by the

user to access a merchant server web site as indicated by 302. In step 602, the user selects goods and/or services from the merchant site and indicates to the site that the user wishes to purchase these items using a stored-value card as indicated at 304. In step 604 the merchant server receives this request for a stored-value card transaction.
In step 606 the merchant server builds an HTML page that includes the following client applet parameters: the total cost of the transaction as determined by the merchant server; the type of currency being used; the port and IP address of the payment server; a unique transaction identifier used by both the payment server and the merchant server to track a transaction; and a unique merchant identifier assigned to the merchant by the acquirer and known to the payment server. Other information may also be included such as the currency's exponent, a status URL address of the merchant server used for communication from the client terminal, and a merchant server generated key and other security information to ensure the identity of the merchant server and the integrity of the message. Other process related information such as software release level, encryption methodology and keys may also be conveyed. Once this page has been built, the page is sent 306 to the requesting client browser and triggers the loading of the client code module (in this example a Java applet) in the client terminal.
Some browsers may not allow an applet to invoke a dynamic link library (DLL) due to security reasons. In an embodiment of the present invention, the client applet along with any DLLs needed are preloaded on the client terminal. Then, the merchant server is allowed to invoke the client applet and DLLs dynamically to circumvent this security precaution.
In step 608 the client module of the client terminal interacts with stored-value card 5 to obtain card information 308 in order to build a draw request message for later transmission 310 to payment server 206. In one embodiment of the invention, the client applet loads a local DLL, makes an API call to that library, which in turn makes a call to another DLL that finally makes a call to the card reader. In this fashion communication with the card is achieved. Once responses from the card are received, the client module will also combine these responses into a byte stream suitable for transmission over a network to a payment server. Also at this point, the currency type and expiration date on the card are checked, and the total cost of the ordered merchandise is checked against the card balance to ensure that the value on the card is great enough to cover the transaction. If the checks are not successful, a message to that effect is delivered to the user and this transaction terminates.
The client module emulates a variety of security card commands to receive responses from these commands from the stored-value card. Because the stored-value card and the security cardare now physically separated from one another, and communication takes place over the Internet, it would not be advantageous to engage in numerous commands and responses over such an open network. In the interest of speed and reliability, it is advantageous to have fewer messages exchanged.
To operate securely and reliably in this environment, in one embodiment of the present invention, client module 224 emulates a security card and gathers all the responses for transmission in one draw request message. The draw request message may include a variety of information including a draw request token, state information, the merchant identifier, the transaction identifier, security information, a purse provider identifier, an intersector electronic purse (IEP) identifier, an algorithm used by the card, an expiry date, the balance of the card, a currency code, a currency exponent, the authentication mode of the IEP, the transaction number of the IEP, a key version and the purchase amount. As all of this information is prepackaged into a single draw request message, the number of messages between the stored-value card and the security card over the Internet is greatly reduced.

In this embodiment, the draw request message is built by packaging the stored-value card's response to the "reset" and "initialize" commands and any public key certificates along with the total cost and the currency of the transaction received from the HTML page. For public key cards, the card and issuer certificates are obtained from read commands and may also be included in the draw request. By packaging all of this information together into one draw request message, it is possible to cut down on the number of messages exchanged between the client server and the payment server, and reliability and speed is improved. In one embodiment of the invention, an intersector electronic purse (IEP) protocol is used to reset and initialize the card and to receive a response.

Next, in step 610 the client terminal accesses the payment server using the IP address received from the merchant server. In step 612 the client terminal sends the draw request message to the payment server as indicated at 310. The client terminal also creates a log of this message being sent.

In step 614 the payment server processes the draw request in conjunction with an associated security card as will be explained in greater detail below with reference to FIG. 11D. Draw request 312 is shown being sent to terminal 214. In one embodiment of the invention, the payment server creates a transaction thread for each connected client module to service it through the life cycle of the transaction. After step 614, the payment server has received a debit command and a security card signature 314 from the security card in the terminal. This debit command may also be termed a "debit IEP" command. The security card signature is a value that uniquely identifies and validates security card 218 to prove to stored-value card 5 that the incoming debit command is a valid command from a real security card. This validation ensures that when the stored-value card is debited, that the financial totals in the security card are updated. Thus, the user of the stored-value card is guaranteed that a valid debit of the card has occurred. In a preferred embodiment of the invention, the security card signature is an encrypted value ensuring that no other entity can forge an identity of a security card.

In step 616 the payment server sends the debit command along with the security card signature to the client terminal as indicated at 316 for the stored-value card to debit itself. At this time, the payment server also logs this debit command into its database.

In step 618, upon receiving the debit command from the payment server, the client module replaces the amount in the debit command with the original amount (from the merchant server) to ensure that the amount has not been tampered with while traveling over the network. At this time, the client module also creates a log of the debit command. Client module 224 then passes 318 the debit command and security card signature to stored-value card 5 which verifies the signature, debits itself by the purchase amount, and also generates a success message (also termed a "debit response" message) and a stored-value card signature. The stored-value card signature is a unique value identifying a valid stored-value card. In a preferred embodiment of the invention, this signature is in encrypted form to prevent tampering. If card 5 does not have enough value to satisfy the purchase amount, then the "debit response" message indicates as such.

In step 620, card 5 sends a success message 320 along with the card signature back to client module 224 in client terminal 204. This success message may also be termed a "debit response" message. At this point, the purchase amount has been deducted from the balance on stored-value card 5. Next, in step 622, client module 224 packages the success message along with the card signature and sends them back to payment server 206 as indicated at 322. Client module 224 also logs the result of this stored-value card debit.

In step 624 the payment server receives incoming message 322 and creates a log and updates the transaction status in its database for future error recovery. The payment server then directs this received message to the security card in the terminal as indicated at 324. Next, in step 626 the security card processes this response from the client's terminal and verifies the received stored-value card signature. As the security card contains the keys and algorithms necessary to compute stored-value card signatures, the security card is able to validate that a received stored-value card signature is in fact a valid one by comparing this stored-value card signature with a generated expected value. A successful comparison indicates that a success message 324 received from the stored-value card is in fact a valid success message and that the stored-value card has been debited. An error result code or a comparison that is not successful potentially indicates that the stored-value card has not been debited by the proper amount. This comparison of stored-value card signatures by the security card ensures that a stored-value card is in fact debited before the merchant server is directed to release the purchased merchandise. This comparison of the stored-value card signature to an expected value is performed by the security card for the highest level of security. As will be described in the embodiments of FIG. 6, 7, and 8, this comparison of stored-value card signatures may also take place in the payment server, in the client terminal or in the merchant server with a variety of other advantages. Assuming that the transaction is so far valid, in step 628 the security

card sends a "confirmation" message back to the payment server as indicated at 326. This confirmation message may also be termed a "message result."

In step 630 the terminal updates its data store with the stored-value card number, a transaction count, the total sale amount, the response from the security card, and transaction numbers from the stored-value card and from the security card. The payment server also logs the response received from the terminal including the merchant identifier, etc., as indicated in step 632. Next, in step 634, the payment server creates a confirmation message including the transaction identifiers and sends this message to the client terminal in encrypted form as indicated at 328. This message 328 may also be termed a "message result."

By sending this confirmation message in encrypted form, the confirmation message may be passed to the merchant server by way of the client terminal without fear of tampering. As the confirmation message is encrypted, it would be extremely difficult for the client terminal or another entity to forge a confirmation message and trick the merchant server into thinking that a transaction had taken place. In another embodiment of the invention, if the client terminal is a trusted agent, then the confirmation message need not be encrypted. In yet another embodiment, the payment server may sent two confirmation messages, one not encrypted for the client to process, and one encrypted for the merchant server. FIGS. 15A and 15B present an embodiment in which the payment server sends two messages to the client terminal.

At this point, the transaction thread of the payment server that was used for the current transaction may release the terminal, thus allowing the terminal to be used by other transactions. This transaction thread then exits at this time.

In step 636 the client terminal then passes this confirmation message 330 on to the merchant server at the URL address previously received from the merchant server. Message 330 may also be termed a "message result." The client may also post a message to the user informing that the debit has been completed. The client also logs confirmation of the payment. In step 638 the merchant server registers this confirmation message and checks for success. The merchant server calls a validate routine within

the merchant code module with the confirmation message in order to validate the response from the client. The validate routine is able to take the transaction identifier along with the encrypted confirmation message to decrypt the confirmation message. If the decrypted confirmation message is acceptable, the merchant server then determines a successful transaction has occurred. Next, in step 640 the merchant server generates an HTML page with the purchased information and delivers this information to the client terminal. Alternatively, the merchant server may generate a purchase receipt to deliver to the client terminal indicating goods and/or services to be rendered. At this point, the client terminal may also log the merchant server's response. Completion of these steps indicates a successful financial transaction over the Internet using a stored-value card.

Returning now to a more detailed discussion of step 614, FIG. 11D describes one technique for processing a draw request message in conjunction with a security card. Once this draw request message has been received by the payment server and passed along to the terminal, the terminal parses the message back into individual responses and passes these responses sequentially to the security card as will be explained below. In an alternative embodiment, a dumb terminal is used and the draw request is parsed into its components and otherwise processed by the payment server, which then sends the responses to the security card itself.

In step 680 the payment code module of the payment server edits the draw request for syntactic correctness and logs the draw request message as being received. In step 682 the draw request is passed to the terminal interface module of the payment server. In one specific embodiment, the terminal interface then requests a terminal from the payment server's terminal pool. The payment server has a pool of terminals connected to the terminal concentrator that is established at start-up. At start-up, the payment server receives a list of all valid terminal identifiers. The payment server uses these identifiers, and its knowledge of transactions in progress to determine an appropriate terminal to process the transaction. Once a terminal is determined, the terminal interface builds a terminal specific message based upon the draw request and the type of terminal.

In step 686 the terminal specific draw request 312 is sent to the chosen terminal via the concentrator over a local area network. The concentrator acts as a router between a transaction thread in the payment server and its corresponding terminal. The concentrator looks at a header on the draw request to determine to which terminal the transaction should be routed. In one embodiment of the invention, concentrator 212 is removed and payment server 206 communicates directly with terminal 214 (for example).

In step 688 the terminal parses the draw request message into its various components and processes each component in turn to emulate a stored-value card interacting with the security card in a physical terminal. Prepackaging of a variety of information into the draw request message results in fewer exchanges over the Internet between the client terminal and the payment server. By now simulating an interaction, the security card behaves as if it were in a physical terminal along with the stored-value card. A variety of responses from a stored-value card may be emulated. In this embodiment, the terminal sends each of the three packages "answer to reset", "initialize IEP", and "debit" down to the security card individually and waits for a return message before sending the next response. For a public key transaction, the certificates read by the client are also included as individual responses. In this fashion, even though all of the stored-value card information (the draw request) originating from the client terminal has been sent at once in prepackaged form over the Internet, the traditional interaction between the

stored-value card and the security card in a physical terminal may be simulated at the terminal in a remote location.

In step 690 the terminal reaches a "draw amount" state, indicating that the security card is able to generate a debit command. In step 692, the security card generates its security card signature and the debit command. The debit command may also be termed a "debit IEP" command. This signature and debit command 314 are sent to the terminal. The debit command issued by the security card may contain a wide variety of information including the security card identifier, the transaction identifier, the amount to be debited, the currency and currency exponent for the amount, the security card signature, the date, time, and location. The terminal in turn, sends the signature, command, and the terminal identifier to the payment server as indicated in step 694. The information may be sent to the payment server as indicated at 314 via a concentrator. At this point, step 614 ends and control returns to step 616.

FIG. 6 illustrates an alternative embodiment 200a in which the security card is able to be released sooner than the security card of FIG. 5; this embodiment also requires fewer exchanges between the terminal and the payment server. A security card in a terminal is dedicated to a particular transaction from the moment when the terminal interface selects that terminal until the security card finally issues a "confirmation" message and is released by a terminal interface. Thus, in some circumstances it is desirable to release the security card earlier. By releasing a security card earlier, the card is tied up for a shorter time per transaction and may move on to the next transaction sooner. Also, the less time that a terminal is dedicated to a particular transaction, and the fewer messages exchanged between the two, the less likely chance there is of a communication error that might interrupt and halt the transaction.

Embodiment 200a includes a client terminal 204, a payment server 206, a merchant server 208, a stored-value card 5, and a terminal 214 having a security card 218. Communication between the various entities may take place in a similar fashion as in FIG. 5 as indicated by communication links 234, 235, and 236. However, instead of two round trips of information between the terminal and payment server, there is only one round trip in this embodiment.

FIG. 12 is a flowchart that describes a technique for implementing this embodiment with reference to FIG. 6. Step 702 indicates that communication between the various entities takes place in a similar fashion as in FIG. 5 up until the terminal reaches the "draw amount" state. At this point, draw request 312 has been received and processed by the security card. Next, in step 704 the security card generates not only the security card signature and the debit command, but also an expected stored-value card signature. This expected stored-value card signature is a value expected by the security card from the stored-value card to validate the stored-value card's success message. This validation will ensure that the stored-valued card has in fact debited itself.

In step 706 the security card signature, the debit command and the expected stored-value card signature are sent to the payment code module in the payment server as indicated at 314a. Also, the terminal updates its data store in a similar fashion as in step 630. Next, step 708

indicates that the transaction occurs as before with reference to step 616-622. The steps indicate that the stored-value card receives the debit command, debits itself, and returns the success message (also termed a "debit response" message) and its card signature to the payment server. Next, in step 710 the payment server code module processes this response from the stored-value card by comparing 346 the received card signature with the expected stored-value card signature received earlier

from the security card. This comparison of the two signatures by the payment module of the payment server foregoes the need for another round trip between the payment server and the security card. Because the security card has already delivered the expected card signature to the payment server, the security card may be released as soon as message 314a is received.

Assuming that the comparison is successful, the payment module is then able to generate its own confirmation message instead of waiting for a "confirmation" message from the security card. Next, step 712 indicates that the processing continues in a similar fashion as in steps 632-640. The confirmation message is passed on to the merchant server by way of the client terminal and the merchant server may then deliver the purchased merchandise to the user.

In another embodiment 200b of the present invention as illustrated in FIG. 7, not only is the security card allowed to release earlier, but the number of messages exchanged between the client terminal and the payment server are reduced. Instead of comparing stored-value card signatures in the payment server, the expected stored-value card signature from the security card is transmitted to the client terminal where a trusted agent 356 performs the comparison of the expected stored-value card signature with the actual signature received from stored-value card 5. Thus, message exchange between the client terminal and the payment server is reduced to one round trip. This is advantageous in that the time for a transaction is reduced, the security card is released earlier and fewer message exchanges means more reliability over the Internet.

Embodiment 200b includes a client terminal 204, a payment server 206, a merchant server 208, a stored-value card 5, and a terminal 214 having a security card 218. Communication between the various entities may take place in a similar fashion as in FIG. 5 as indicated by communication links 234 and 235.

FIG. 13 is a flowchart that describes a technique for implementing this embodiment with reference to FIG. 7. Step 722 indicates that communication between the various entities takes place in a similar fashion as in FIG. 5 up until the terminal reaches the "draw amount" state. At this point, draw request 312 has been received and processed by the security card. Next, in step 724 the security card generates not only the security card signature and the debit command, but also an expected stored-value card signature.

In step 726 the security card signature, the debit command and this expected stored-value card signature are sent to the payment code module in the payment server as indicated in 314a. Also, the terminal updates its data store in a similar fashion as in step 630. Next, in step 728 the payment server code module sends the debit command, merchant signature and expected stored-valued card signature to the client terminal.

Next, step 730 indicates that the transaction occurs as before with reference to steps 618 and 620. The steps indicate that the stored-value card receives the debit command and debits itself. In step 732, the client code module itself compares the actual card signature from the stored-value card with the expected signature from the security card. This comparison of the two signatures by the client module of the client terminal foregoes the need for another round trip between the payment server and the client terminal. Also, because the security card has already delivered the expected card signature to the payment server, the security card may be released as soon as message 314a is received.

Assuming that the comparison is successful, the client terminal is then able to generate its own confirmation message in step 734 instead of waiting for a confirmation message from the payment server. Next, step 736 indicates that the processing continues in a similar fashion as in steps 636-640. The confirmation message is passed on to the merchant server and the merchant server may then deliver the purchased merchandise

to the user.
FIG. 8 illustrates another embodiment 200c of the invention in which the merchant server performs the comparison of the stored-value card signature with the expected signature. This embodiment has all of the advantages of the previous embodiment in which the security card is released earlier, and there are also fewer messages passed between the entities. In this embodiment, if the client terminal is not to be trusted to compare the stored-value card signatures, then an encrypted signature is passed to the merchant server via the client terminal. The client terminal also passes the raw, unencrypted signature from the stored-value card to the merchant server. A routine 366 in the merchant server then compares the two signatures.
Embodiment 200c includes a client terminal 204, a payment server 206, a merchant server 208, a stored-value card 5, and a terminal 214 having a security card 218. Communication between the various entities may take place in a similar fashion as in FIG. 5 as indicated by messages 302-306 and communication link 235.
FIG. 14 is a flowchart that describes a technique for implementing this embodiment with reference to FIG. 8. Step 742 indicates that communication between the various entities takes place in a similar fashion as in FIG. 5 up until the terminal reaches the "draw amount" state. At this point, draw request 312 has been received and processed by the security card. Next, in step 744 the security card generates not only the security card signature and the debit command, but also an expected stored-value card signature.
In step 746 the security card signature, the debit command and this expected stored-value card signature are sent to the payment code module in the payment server as indicated in 314a. Also, the terminal updates its data store in a similar fashion as in step 630. Next, in step 748 the payment server code module sends the debit command, merchant signature and an encrypted expected stored-valued card signature to the client terminal. The expected stored-valued card signature is encrypted to prevent tampering by the client terminal or other outside entity.
Next, step 750 indicates that the transaction occurs as before with reference to steps 618 and 620. The steps indicate that the stored-value card receives the debit command and debits itself. In step 752, the client code module sends the success message, the raw stored-value card signature and the encrypted signature on to the merchant server. In step 754 the merchant server processes the success message, decrypts the encrypted signature, and compares the two signatures. This comparison of the two signatures by the merchant server foregoes the need for another round trip between the payment server and the client terminal. Also, because the security card has already delivered the expected card signature to the payment server, the security card may be released as soon as message 314a is received.
Assuming that the comparison is successful, the merchant server is then able to generate its own confirmation message in step 756 instead of waiting for a confirmation message from the client terminal. Next, step 758 indicates that the processing continues in a similar fashion as in steps 638 and 640. The merchant server may then deliver the purchased merchandise to the user. In all of the above alternative embodiments, when the transaction is not completed successfully, the payment server reverses the transaction within the terminal.
FIG. 9 illustrates an embodiment 200d of the present invention in which an encryption layer has been added. Although the present invention may be practiced without this added encryption layer, in a preferred embodiment of the invention, this encryption layer is used. FIG. 9 includes client terminal 204, payment server 206 and merchant server 208. Other elements of the architecture have been omitted in this figure for simplicity. This extra encryption layer is used not only to protect the contents of

messages being transmitted over the Internet, but also to prevent a client terminal, stored-value card or other entity from receiving or producing a message that would trick another entity into thinking that a valid transaction had occurred. This encryption also prevents messages from being accidentally or deliberately altered or misdirected.
It should be appreciated that encryption may be present in any embodiment on all parts of any message sent for security. Preferably, any signature sent over a network is encrypted.
Figures 15A and 15B are a flowchart describing this embodiment of the invention with reference to FIG. 9. In step 802, the payment server and the merchant server share a unique encryption key. Through a prior business arrangement, both of the servers have arranged to share this unique key to add security to the transaction. The shared key may be of any suitable encryption standard and of any length. The key may be a Data Encryption Standard (DES) key having a length of 128 bits including parity. Although this shared key could be used directly, in a preferred embodiment of the invention, there is a derived unique key for each transaction between the merchant server and the payment server.

Alternatively, another encryption standard such as RSA may also be used. Preferably, loading of value is performed under DES, while a purchase may be performed under either DES or public key technology.
In step 804 the client terminal and the merchant server engage in a protected Secure Sockets Layer (SSL) session 404 in which a connection is made, a user browses and makes a purchase selection. The SSL session protects the information transmitted over the Internet such as card information, commands, and encryption keys from being discovered by an unauthorized party. Other techniques for protecting a session may also be used.
In step 806 the merchant server derives a key from the DES key using information unique to the transaction such as the merchant identifier, the transaction identifier, or other information unique to this transaction, such as a random number. Because the payment server shares the DES key with the merchant server and also has access to this unique information about the transaction, the payment server will also be able to derive this same key from the shared DES key. In this step the merchant server also creates a transaction session key (TSK) for use by the client terminal and payment server in encrypting information.
In step 808 the merchant server downloads an HTML page of information 406 that includes the TSK and the TSK that is encrypted using the derived key (ETSK). The TSK encrypted with the derived key will be used by the payment server to return an encrypted (and unreadable by the client) confirmation message to the merchant server. Only the merchant server will be able to decrypt this confirmation message and will thus be guaranteed that a successful transaction has occurred and that merchandise may be released to the client.
In step 810, the client prepares the draw request in conjunction with the stored-value card and sends the draw request 408 encrypted with the TSK to the payment server along with the ETSK. In step 812 the payment server uses the shared DES key and the prearranged information unique to the transaction to derive the same key that the merchant server has used. Thus, the derived key can be used to decrypt the ETSK in order to produce the TSK. Once the payment server had produced the TSK, it may decrypt the draw request and process the draw request in any suitable fashion with the security card. Once the payment server has received the debit command from the security card, it encrypts the debit command with the TSK. The

debit command may also be termed the "debit IEP command."
In step 814 the payment server sends the encrypted debit command 410 to the client terminal. In step 816 the client decrypts the debit command

with the TSK it had received earlier from the merchant server and processes the debit command in a suitable fashion with a stored-value card. Once the client terminal has received the debit response message from the stored-value card, it encrypts this message with the TSK and sends the debit response message 412 to the payment server. In step 820, the payment server decrypts the debit response message with the TSK and processes the debit response message in a suitable fashion with the security card.

Once the payment server has received a "debit result" message from the security card, the payment server encrypts the "debit result" message with the TSK to form a "debit result C" message for the client. The "debit result C" message will be used by the client terminal to inform the user of a successful transaction. The payment server also generates its own confirmation message and encrypts the confirmation message with the derived key to form a "debit result M" message. The payment server then sends 414 the "debit result C" message and the "debit result M" message to the client terminal.

In step 822 the client terminal decrypts and processes the "debit result C" message and passes the "debit result M" message 416 on to the merchant server. Because the "debit result M" message is encrypted with the derived key, the client terminal or other entity is not able to tamper with it. In step 824 the merchant server is able to decrypt the "debit result M" message because it had originally produced the derived key from the DES key. Once the merchant server has determined that a valid "debit result M" message has been received, it confirms that a valid transaction has taken place and may release merchandise to the user.

This security embodiment of FIG. 9 may be used with any of the previously described embodiments of the invention. By way of example, this security embodiment may be used with the embodiments of Figures 7 and 8 in which there is only one round trip between the client terminal and the payment server. In particular, the expected stored-value card signature received from the security card may be encrypted with the derived key so that it unreadable by the client, yet the merchant server will be able to compare the received stored-value card signature with the expected card signature to validate the transaction.

A wide variety of terminology may be used to describe the keys described above. For example, the keys referred to above as shared DES key, transaction session key (TSK) and derived key, may also be referred to as shared key, session C key and session M key.

FIG. 16 illustrates an architecture and system 200' for authentication over an internet (such as the Internet) using a pseudo stored-value application. This application could reside on a stored-value card along with standard accounts, stored value, or other card applications. The card defines access to the pseudo stored-value service and ensures that the card is present and passes security checks.

In one embodiment of the present invention, a consumer may wish to access any of a variety of Web servers in order to redeem **frequent flyer miles** , award points, etc., that he or she has **accumulated** . In this embodiment, a consumer has accumulated "points" through any of a variety of programs with airlines, restaurants, rental car companies, hotels, banks, **credit** or debit card issuers, telephone or other communication **company** , etc. The consumer wishes to redeem these points to receive free airline tickets, meals, car rental, overnight stays, prizes, awards, discounts, or other "benefits". By accessing a Web server associated with the particular program, the consumer is able to use his or her card in any of the embodiments described herein to authenticate the card and to receive these benefits from the program. Most often, a card has a card number that is associated with the consumer's name in a database on the Web server. This card number is transmitted to the Web

server as part of the card signature, or in a similar fashion. Thus, an authenticated card used in this embodiment to redeem services may be matched to the appropriate consumer.

For example, a consumer with 30,000 frequent flyer miles on one airline may use this embodiment of the present invention to access a Web server associated with the airline. The consumer is requesting a free round-trip ticket in exchange for 20,000 miles. The present invention then operates to authenticate the consumer's stored-value loyalty application on the card, and delivers a confirmation of authentication message to the Web server for the airline. The Web server then deducts 20,000 miles from the consumer's account (leaving 10,000 miles) and delivers the free ticket to the consumer. In one specific embodiment, the Web server associated with the airline (or the airline itself) keeps track of the consumer's account and deducts the mileage. In this instance, an authentication application is used to validate the presence of the card or to obtain access to the Web server site.

In another specific embodiment, the consumer's card contains a loyalty application that stores the consumer's accumulated frequent flyer mileage; the mileage from the card is then debited and confirmed to the Web server in a similar fashion as described in various of the embodiments by which a cash value is stored on and debited from a card.

System 200' may be implemented in a similar fashion as system 200 of FIG. 4. The elements shown in system 200' having counterparts in system 200 are described above and have similar functionality. System 200' includes a web server 208' that may be any suitable computer server capable of presenting award information (hereinafter "benefits") to a consumer over an open network such as the Internet. Web server 208' may be the same as merchant server 208 of FIG. 4 or a separate computer. Preferably, web server 208' is implemented in a similar fashion as described above for merchant server 208. Web server 208' includes server module 232' that is preferably implemented in a similar fashion as merchant module 232. Additionally, server module 232' includes functionality to store and present benefits that are available for particular consumers. For example, benefits available such as airline tickets, prizes, etc., may be presented.

Points (such as frequent flyer miles, for example) that a consumer accumulates to achieve benefits may be linked to a particular consumer by an account number, password, or other identifier. The amount of points accumulated for each consumer may be stored on web server 208' using server module 232', or may be located in another database of the organization providing the benefits. In an alternative embodiment, these points for each program that a consumer is enrolled in are stored in a loyalty application on the consumer's card. For example, a consumer may have a stored-value card that in addition to storing monetary value, also stores a quantity of frequent flyer miles accumulated for a particular airline (or a number of airlines), points accumulated for using a particular credit card, points for hotel stays at particular hotels, etc. For points stored on the consumer's loyalty application card, these

points may be verified and debited in much the same way that monetary value on the consumer's card is debited as described herein.

One embodiment by which a consumer has his or her pseudo stored-value application on a card authenticated to redeem points for benefits will now be explained. In one specific embodiment, a technique similar to that described in the flowchart of FIGS. 11A-11D for debiting monetary value may be used. Initially, a user (consumer) operating client terminal 204 accesses web server 208' over link 234', views benefits presented for a particular program (such as an airline's frequent flyer program), selects benefits from that program, and requests the transaction to be performed using his or her pseudo stored-value application to validate that the

card has access to the services. Web server 208' receives and processes this request. The above steps may be performed in a similar fashion as steps 602 and 604.
Next, similar to step 606, web server 208' sends a page of information to client terminal 204. When claiming benefits, the total cost field is zero and the currency field is a specially assigned value. Keeping total cost field equal to zero causes the system to perform authentication but not to create a payment record. Alternatively, for those user's whose card holds the amount of their points, additional fields may be sent from server 208' to terminal 204 indicating which account to debit and by how many points. The total cost and currency fields may be readily adapted for this purpose.
Next, in a similar fashion to steps 608 - 612, a draw request message is built, and the draw request is sent to authentication server 206' over link 236'. Similar to step 614, the authentication server now processes the draw request in conjunction with security card 218 (for example) and sends back a "debit" command and a security card signature to authentication server 206'. As total cost is zero, the "draw amount" state reached by security card 218 is also zero. In the alternative embodiment in which stored-value card 5 stores points for a particular program, total cost may be a value and a "draw amount" state may be reached indicating a number of points to be deducted from card 5.
Next, similar to steps 616-618, authentication server 206' sends the debit command and security card signature to client terminal 204 and this information is processed by card 5. Even though a monetary value is not being debited, card 5 performs processing such as incrementing a counter indicating number of transactions and generating a stored-value card signature. In the alternative embodiment in which points are stored on card 5, the points needed to redeem the benefit chosen by the user from web server 208' may be debited from the appropriate account in this step.

Steps 620 through 638 are performed in a similar manner as in FIGS. 11B and 11C, except that in this case a monetary transaction is not being verified, but rather card 5 is being authenticated to allow the user to complete his access to services or benefits. In step 626 in particular, the signature of card 5 is verified by security card 218. In this embodiment, security card 218 would send an "authentication OK" message rather than the "confirmation" message of step 628. Web server 208' then debits the appropriate number of points from the user's account or allows access to a privileged service for the benefit requested. In the alternative embodiment in which points are stored on card 5, the "authentication OK" message serves not only as an authentication of card 5, but also confirmation that the correct number of points have been debited from card 5 for the appropriate program. Next, similar to step 640, web server 208' releases the benefit requested by the user (such as airline tickets, prizes, discounts, etc.) and the benefit is arranged to be delivered to the user.
It should be appreciated that this technique of redeeming points for benefits may also be practiced using any of the alternative embodiments of FIGS. 6, 7 or 8, thereby obtaining the advantages associated with those embodiments. Furthermore, this technique may take advantage of the encryption layer embodiment of FIG. 9. Additionally, as described below, the present invention may also be used to load more points onto card 5 in much the same way that monetary value is added.
FIG. 17 illustrates a system 850 for loading value onto a stored-value card according to one embodiment of the present invention. System 850 includes a client terminal 204, bank server 860 and load server 862. Client terminal 204 communicates with card 5 via card reader 210, and with bank server 860 and load server 862 over any suitable open network such as Internet 202. Suitable embodiments for the client terminal, the

card reader and the stored-value card are described above in the description of a payment technique. Preferably, each of client terminal 204, bank server 860 and load server 862 implement a code module (similar in operation to the code modules described above) in the Java programming language that provides the functionality described below. For simplicity of explanation, reference will be made below to "client terminal", "bank server" and "load server" even though the resident code is performing the functions. Card issuer 108 has been described previously in FIG. 3. Card issuer 108 may be a separate financial institution from the bank that includes bank server 860, or card issuer 108 may be the same bank that includes bank server 860.

Bank server 860 is any suitable computer within a bank or other financial institution. By way of example, bank server 860 is any suitable personal computer, a workstation or a mainframe computer. In one embodiment, bank server 860 runs a "servlet" program (a Java applet running on server) for communication with client 204.

Load server 862 is also any suitable computer and may be located at a third party location (such as at a processor) or may be located within the same bank as bank server 860. Load server 862 also runs a servlet program for communication with client terminal 204 and host security module 864. In an alternative embodiment, load server 862 and bank server 860 are the same computer which runs two different applications representing the functionality of each server.

Host security module (HSM) 864 is a device known in the art that may be embodied in a hardware "black box" or on any suitable computer. The host security module can be implemented in a hardware module outside of load server 862, can be implemented within load server 862, can be implemented in software, or can be implemented as a security card described above. Host security module 864 contains the encryption keys in hardware used for generating signatures (for example S1, S2 and S3) that provide security for the transaction. These signatures are used by stored-value card 5 and host security module 864 to insure that the card is not expired or counterfeit (i.e., is a valid card), to insure that module 864 is authentic, to insure that system 850 is authentic and, in general, to provide for a valid transaction and to prevent fraud. Card 5 also includes encryption keys for the generation of a stored-value card signature. In an alternative embodiment, module 864 could be replaced by a standard terminal that includes a security card such as is shown in the previous embodiments. In this situation, the encryption keys would be stored in the security card.

Briefly, system 850 operates as follows. A consumer accesses bank server 860 via client terminal 204. Assuming that card 5 is not overloaded and that the user's account with the bank has sufficient funds, the user is able to download value via bank server 860 on to his stored-value card 5. Client terminal 204 communicates with load server 862 to receive authorization for the load and for higher security. Card 5 may then be used to make purchases over the Internet as described earlier in the application or may be used for purchases elsewhere. Once the bank has downloaded value to card 5, a corresponding amount of funds is transferred from the bank to card issuer 108.

Card issuer 108 places these funds in a holding pool. Once stored-value card 5 is used to make a purchase from a merchant, the transaction is captured and settled through a settlement service, such as VisaNet. The issuer bank decrements the funds pool for the amount of the purchase, which is paid to the merchant bank. The merchant bank pays the merchant for the transaction. Settlement may occur in any suitable fashion such as is known in the art and, in particular, may be implemented as previously described in FIG. 3.

One embodiment of a technique by which a stored-value card is loaded over the Internet will now be described using the flowchart of FIGS. 18A

through 18D with reference to FIG. 17. Various of the steps below may occur in a different order; the following description is for illustration purposes. Interaction between client terminal 204 and bank server 860, and between client terminal 204 and load server 862, is preferably implemented in a similar fashion as between client terminal 204 and merchant server 208, and between client terminal 204 and payment server 206 as described above, respectively. Certain implementation details mentioned above with respect to payment are equally applicable to loading a stored-value card. Furthermore, the exemplary flow shown in the figures illustrates a successful transaction (although a negative result is also explained below in the text). For this reason, a "confirmation" message is referred to, which can more broadly be referred to as a "result" message (to reflect both the possibilities of success and failure of a load). Also, a "load success" message is referred to, which can also be

referred to as a "confirmation" message, to reflect its status as either confirming a positive load result or a negative load result.

Initially, a suitable web browser of client terminal 204 is used by the user to access a bank server Internet site. In step 871 the user selects an option to load value onto card 5. In step 872 the bank server sends a request for card information (including current card balance and maximum card balance); client terminal 204 reads the current card balance, currency, and other card information via card reader 210 and returns the balance to bank server 860. In step 873 the bank server determines the maximum load value and verifies that enough funds are in the user's account to accommodate a load request.

In step 874 the bank server builds an HTML page that includes the following client applet parameters: the load value; the type of currency being used; the port and IP address of the load server; a unique transaction identifier used by both the load server and the bank server to track a transaction; a unique bank identifier assigned to the bank and known to the load server; and a session key. Other information may also be included such as the currency's exponent, a status URL address of the bank server used for communication from the client terminal, and other security information to ensure the identity of the bank server and the integrity of the message. Other process related information such as software release level, encryption methodology and keys may also be conveyed. Once this page has been built, the page is sent to the requesting client browser and triggers the activation of the client code module (in this example a Java applet) in the client terminal.

To determine the load value, the bank server requests that the user enter the amount to load to the card. Assuming that the user's account is adequate, the bank server requests the user's account be debited in step 875 by the load value. Advantageously, the debit request from the bank server can use the existing ATM and accounting systems of the bank to debit the user's account. From the bank's point of view, value is being transferred from the user's account much in the same way that value would be transferred to a user in the form of cash at an ATM. In this situation, though, the value is not being dispensed as cash at an ATM, but is being sent over the Internet to a stored-value card.

In step 876 the client terminal interacts with stored-value card 5 to obtain card information in order to build a load request message for later transmission to load server 862. Once responses from the card are received, the client terminal combines these responses into a byte stream suitable for transmission over a network to a load server.

The client terminal emulates a variety of host security module 864 commands to receive responses from these commands from the stored-value card. The stored-value card and the security module are physically separated from one another; communication takes place over the Internet. In the interest of speed and reliability, it is advantageous to have only

the traditional authentication, response, and confirmation messages exchanged.
To operate securely and reliably in this environment, in one embodiment of the present invention the client terminal emulates a security module and gathers all the responses for transmission into one load request message. The load request message may include a variety of information and preferably includes a first card signature (termed S1), a card number, an expiry date, and a load amount. Other information such as the security algorithm, transaction counter, current card balance, and bank server time stamp are also preferably provided.
As all of this information is prepackaged into a single load request message, the number of messages exchanged between the stored-value card and the security module over the Internet is minimized.
Next, in step 877 the client terminal accesses the load server using the IP address received from the bank server. In step 878 the client terminal sends the load request message to the load server. In step 879 the load server processes the load request in conjunction with an associated host security module 864 as will be explained in greater detail below with reference to FIG. 18D. After step 879, the load server has received an issuer security module signature (termed S2) as part of a load command from the security module 864. The security module signature is a value that uniquely identifies and validates the security module to prove to stored-value card 5 that the incoming load command is a valid command from a real security module. Thus, the user of the stored-value card, and other interested parties are guaranteed that a valid load of the card has occurred. In a preferred embodiment of the invention, the security module signature is an encrypted value ensuring that no other entity can forge an identity of a security module.
In step 880 the load server sends the load command including with the security module signature to the client terminal for the stored-value card to load itself. In step 881, upon receiving the load command from the load server, the client terminal passes the load command to stored-value card 5 which verifies the signature, loads itself by the load value, and also generates a load success message, a second stored-value card signature (termed S3), and a result code indicating success or failure of the load. In a preferred embodiment of the invention, this signature is in encrypted form to prevent tampering.
In step 882, card 5 sends load success message containing the card signature (S3) and result code back to client terminal 204. Next, in step 883 client terminal 204 packages the load success message along with the card signature and sends them back to load server 862. In step 884 the load server receives the incoming message. The load server then processes the message into its components and directs the components to the security module. Next, in step 885 the security module may process this response from the client's terminal and verify the received stored-value card signature (S3).
As the security module contains the keys and algorithms necessary to compute stored-value card signatures, the security module is able to validate that a received stored-value card signature is in fact a valid one by comparing the received stored-value card signature with a generated expected value. A successful comparison indicates that a load success message received from the stored-value card is in fact a valid success message and that the stored-value card has been loaded. Assuming that the transaction is so far valid, in step 886 the security module sends a "confirmation" message back to the load server.
It is possible that the stored-value card has not been loaded by the proper amount, that the card is invalid, a user is fraudulent or another discrepancy. For example, it is possible that a user has tampered with the card to make it appear that a load has not occurred, when in fact a load has occurred. In this situation, processing in step 882 and on is

slightly different. For example, instead of generating a "load success" message, the card my generate a "negative result" code, potentially indicating that the card has not been loaded. Processing of this situation would then occur as follows.

In step 882, card 5 sends a load message containing the result code and stored-value card signature S3 back to client terminal 204. Client terminal 204 recognizes a negative result code, and invokes negative result handling. Client terminal 204 interacts with card 5 and generates a new load request for a zero value load using elements from the original request, along with a new card signature S1.

The negative result code, along with the signatures S3 and new S1, and the zero value load request are passed to the load server for analysis. The load server determines if the transaction counter in the zero value load equals the transaction counter in the previous request, along with verifying other pertinent information such as date and time, card number, and currency code and exponent. If the transaction counters are the same, then it is possible that a valid negative result has been received, but it should be verified because the client is not trusted. If the counters are equal, the load server will hold the original S3 and will generate a new load request to the security module using data element values that would have been expected if the original transaction had failed. The new load request along with the new S1 is sent to the security module. The security module then compares the original S1 (from the original load request) to the new S1. If S1 is valid, then the original negative result is true and the security module generates a signature to confirm to the load server that there was no load. The original negative result from the card is then released to the security module to complete the original transaction. Processing would continue, but a user account would not be debited, and no settlement need occur because the card was, in fact, not loaded. If S1 is not valid, the negative response is not true and then the result code in the original request is changed to reflect a successful load and passed to the security module. Processing then continues reflecting that a load has occurred.

On the other hand, if the transaction counters are not the same, then it is still possible that a valid negative result has been received, but it should be verified because the client is not trusted. First, the load server decreases the transaction counter in the new load request to match that of the original. The request along with the new S1 is passed to the security module. The security module calculates its own new S1 based upon the modified new load request. If there is no match, it means that the negative result was in error and that the card had been loaded. Processing continues to reflect a loaded card. If there is a match, it means the negative result was correct and that the transaction counter had been increased by accident. The user account is not debited, and not settlement occurs.

Returning now to further processing, in step 887 the load server logs

the response received from the security module and updates its database with the transaction identifier, the bank identifier, the load value, etc. In general, any of the plethora of information passing through the load server may be added to its database. Next, in step 890 the load server creates a confirmation message including the transaction identifier and sends this message to the client terminal in encrypted form. By sending this confirmation message in encrypted form, the confirmation message may be forwarded to the bank server by way of the client terminal without fear of tampering. As the confirmation message is encrypted, itwould be difficult for the client terminal or another entity to forge a confirmation message and trick the bank server into thinking that a valid load had taken place.

In step 891 the client terminal forwards the confirmation message on to

the bank server at the URL address previously received from the bank server. The client terminal may also post a message to the user informing that the load has been completed. The client terminal also logs confirmation of the load. In step 892 the bank server registers the confirmation message. The bank server calls a routine to decrypt the confirmation message. If the decrypted confirmation message is acceptable, the bank server determines a successful load has occurred. The confirmation message provides assurance to the bank that the user's card was in fact loaded with a particular value and prevents fraud. For example, a fraudulent user who tries to claim that his bank account was decremented and his card not loaded (and should thus receive more money from the bank) would be thwarted because the confirmation message proves that the user's card was in fact loaded. Alternatively, the "confirmation" message may indicate that a load did not occur, in which case the account would not be debited, and no settlement would occur. At this point a successful load of the user's card has occurred (assuming all is well). For example, if the user had requested $100, that amount has been decremented from the user's account at the bank, and $100 has been loaded onto the user's stored-value card. Preferably, at this point the amount loaded (in this example $100) is transferred from the bank to the stored-value card issuer preferably through an existing network. The $100 is transferred so that the card issuer may manage the float on these unspent funds until the user spends the $100. Once the $100 (or a smaller portion) has been spent with a merchant, the card issuer is then able to settle the transaction with the merchant using any suitable clearing and administration system. In alternative embodiment, the bank may retain the $100 and settle directly with the merchant. In another embodiment, the bank and the card issuer are the same financial institution, and the $100 may be shifted between parts of the organization or remain in place.

Returning now to a more detailed discussion of step 879, FIG. 11D describes a technique for processing a load request message in conjunction with a security module. Once the load request message is received by the load server, the load server parses it into the appropriate elements and passes a request to the security module as will be explained below. Alternatively, the load server can build a network message and switch the request to a remote authentication server. Or, a smart terminal could parse the message and pass responses to the security module.

In step 895 the load server edits the load request for syntactic correctness and logs the request as received. In step 896 the load server constructs a load request message. In step 897 the load server passes the load request to the security module to emulate a stored-value card interacting with the security module. The load server behaves as if a stored-value card were actually interacting in an ATM (for example) through a network to a host with a security module. In this fashion, the load request originating from the client terminal has been sent in prepackaged form over the Internet emulating a traditional interaction between the stored-value card in an ATM.

In step 898, the security module verifies the received stored-value card signature (S1) to prevent fraud. The security module generates its security module signature (termed S2) and the load command. The signature S2 will confirm to the client terminal and the stored-value card that the host security module is authentic and belongs to the issuer of the stored-value card. Additionally, S2 protects against a user trying to perform a fake load, keys out of synchronization, a counterfeit card, an expired card, etc. The security module then sends the signature and load command to the load server as indicated in step 899. At this point, step 879 ends and control returns to step 880.

In another embodiment of the loading technique, a consumer may wish to

access any of a variety of Web servers in order to load frequent flyer miles, award points, etc., that he or she has accumulated. A technique for authentication and redemption of such "points" is described above. In the loading embodiment, a consumer has accumulated points through any of a variety of programs with airlines, restaurants, rental car companies, hotels, banks, credit or debit card issuers, telephone or other communication companies, etc. These points are stored by the particular airline, etc., that has issued them. The consumer wishes to load these points onto his or her stored-value card in order to redeem them elsewhere; thus receiving airline tickets, meals, car rental, overnight stays, prizes, awards, discounts, or other benefits. By accessing an Internet server associated with the particular program, the consumer is able to load his or her stored-value card in any of the embodiments described herein to receive the benefits of the program, much in the same way that currency is loaded.

FIG. 19 illustrates a computer system 900 suitable for implementing an embodiment of the present invention. Computer system 900 includes any number of processors 902 (also referred to as central processing units, or CPUs) that are coupled to storage devices including primary storage 906 (such as random access memory, or RAM) and primary storage 904 (such as a read only memory, or ROM). As is well known in the art, primary storage 904 acts to transfer data and instructions uni-directionally to the CPU and primary storage 906 is used typically to transfer data and instructions in a bidirectional manner. Both of these primary storage devices may include any suitable of the computer-readable media described below. A mass storage device 908 is also coupled bi-directionally to CPU 902 and provides additional data storage capacity and may also include any of the computer-readable media described below. Mass storage device 908 may be used to store programs, data and the like and is typically a secondary storage medium (such as a hard disk) that is slower than primary storage. It will be appreciated that the information retained within mass storage device 908, may, in appropriate cases, be incorporated in standard fashion as part of primary storage 906 as virtual memory. A specific mass storage device such as a CD-ROM 914 passes data uni-directionally to the CPU.

CPU 902 is also coupled to an interface 910 that includes one or more input/output devices such as such as video monitors, track balls, mice, keyboards, microphones, touch-sensitive displays, transducer card readers, magnetic or paper tape readers, tablets, styluses, voice or handwriting recognizers, biometrics readers, or other computers. CPU 902 optionally may be coupled to another computer or telecommunications network using a network connection as shown generally at 912. With such a network connection, it is contemplated that the CPU might receive information from the network, or might output information to the network in the course of performing the above-described method steps. Furthermore, method embodiments of the present invention may execute solely upon CPU 902 or may execute over a network connection such as the Internet in conjunction with a remote CPU that shares a portion of the processing.

In addition, embodiments of the present invention further relate to computer storage products with a computer readable medium that have program code thereon for performing various computer-implemented operations. The media and program code may be those specially designed and constructed for the purposes of the present invention, or they may be of the kind well known and available to those having skill in the computer software arts. Examples of computer-readable media include, but are not limited to: magnetic media such as hard disks, floppy disks, and magnetic tape; optical media such as CD-ROM disks; magneto-optical media such as floptical disks; and hardware devices that are specially configured to store and execute program code, such as

application-specific integrated circuits (ASICs), programmable logic devices (PLDs) and ROM and RAM devices. Examples of program code include machine code, such as produced by a compiler, and files containing higher level code that are executed by a computer using an interpreter. Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be practiced. For instance, any suitable stored-value card capable of loading, storing and decrementing value on command may be used with the present invention. Also, any network capable of performing routing functionality between a client terminal and a load and bank server may be used. Furthermore, the security module may be a physically separate module, a card located in a terminal attached to a load server, or its functionality may be incorporated directly into a load server in hardware or software. And although the client terminal may be used to route messages between the bank server and load server, both

of these servers may also communicate directly between themselves, and may even be the same computer. The specific messages shown passing between the computers are exemplary, and other types of messages may be used. A specified load request is shown, but other information may also be loaded onto a stored-value card using a security module emulation and then sent packaged as one message to the security module over a network. In addition to monetary value, other types of value such as electronic cash, checks, awards, loyalty points, benefits, etc., may be loaded onto a card, and the term "value" is intended to broadly cover all these various types. Any suitable type of encryption may be used to encrypt messages passing between the computers.

CLAIMS 1. A loading system for loading value over a network onto a stored-value card, said loading system comprising:
a router for routing communication between entities attached to said network;
a bank server in communication with said network, said bank server arranged to debit a user account by an indicated value;
a client terminal in communication with said network, said client terminal including a card reader for communicating with a stored-value card and an input device for indicating a value to debited from said user account; and
a load server in communication with said network, said load server including an interface for communicating with a security module and being arranged to receive a load request including a stored-value card signature and being further arranged to transmit a confirmation message to said bank server over said network, thereby assuring that said stored-value card has been loaded by said indicated value.
2. A loading system according to claim 1, wherein said network is an internet and said bank server includes a bank web site for accepting a load request.
3. A loading system according to claim 1 or 2, wherein said client terminal and said bank server are at separate locations and communicate over said internet.
4. A loading system according to any preceding claim, further comprising:
a clearing and administration system for reconciling said debit of said user account with a purchase using said stored-value card.
5. A loading system according to any preceding claim, wherein said client terminal further includes a command emulator for emulating security module commands that are sent to said stored-value card and for grouping responses to said security module commands into a load request message to be sent to said load server, and wherein said load server includes a response emulator for emulating responses from said

stored-value card that are sent to said security module.
6. A loading system according to any preceding claim, wherein said security module includes a comparator for comparing a stored-valued card signature received from said stored-value card with an expected signature to confirm a transaction.
7. A computer-implemented method of loading a stored-value card over a network comprising the steps of:
establishing communication between a bank server and a client over a network;
receiving a request from said client to load value onto a stored-value card;
transmitting to said client a verified load value so that said client may load a stored-value card associated with said client by said load value;
transmitting to said client an address of a load server so that said client may send a load request to said load server; and
a confirmation step for performing the function of confirming the loading of said stored-value card, whereby said bank server is assured that the loading is a success.
8. A method according to claim 7, wherein said network is an internet over which said recited steps of said method occur, wherein said bank server includes a bank web site for accepting a load request, and wherein said client and said bank server are at separate locations.
9. A method according to claim 7 or 8, wherein said confirmation step includes receiving a confirmation message that originates from one of said load server and a security module associated with said load server.
10. A method according to any of claims 7 to 9, further comprising the steps of:
transmitting a first key to said client for encrypting a load request to be sent to said load server;
providing said first key to decrypt said encrypted load request to said load server without sending said first key in the clear to said load server; and
receiving an encrypted confirmation message from said load server that is encrypted by a second key shared between said bank server and said load server.
11. A method according to any of claims 7 to 10, further comprising the steps of:
debiting a user account by said load value; and
sending transaction information including said load value to a stored-value card issuer for later settlement.
12. A computer-implemented method of loading a stored-value card over a network comprising the steps of:
transmitting over a network from a client terminal to a bank server a request to load a stored-value card;
receiving from said bank server a verified load value;
sending a load request to a load server connected to said network;
receiving a load command from said load server;
loading said stored-value card by said load value; and
sending confirmation information to said bank server, whereby said bank server is assured that said loading is a success.
13. A method according to claim 12, wherein said network is an internet over which said recited steps of said method occur, wherein said bank server includes a bank web site for accepting a load request, and wherein said client terminal and said bank server are at separate locations.
14. A method according to claim 12 or 13, further comprising the steps of:
emulating security module commands that are sent to said stored-value

card associated with said client terminal; and
grouping responses to said security module commands into said load request so that said responses may be sent as a group to said load server to reduce network traffic between said load server and said client terminal.
15. A method according to any of claims 12 to 14, wherein said confirmation information includes an encrypted confirmation message unreadable by said client terminal, said method further comprising:

receiving said encrypted confirmation message from said load server.
16. A computer-implemented method of managing a stored-value card load transaction between a client terminal and a bank server connected over a network, said method comprising the steps of:
receiving by a load server over said network a load request, said load request including a stored-value card signature;
sending said stored-value card signature to a security module associated with said load server so that said stored-value card signature may be validated by said security module;
receiving a load command from said security module;
sending said load command from said load server destined to said client terminal so that a stored-value card associated with said client terminal may be loaded by a load value; and
a confirmation step for performing the function of confirming the loading of said stored-value card, whereby a bank server is informed that the loading is a success.
17. A method according to claim 16, wherein said network is an internet over which said recited steps of said method occur, wherein said bank server includes a bank web site for accepting a load request, and wherein said client terminal and said bank server are at separate locations.
18. A method according to claim 16 or 17, further comprising the steps of:
receiving as part of said load request responses from said stored-value card to security module commands that have been emulated by said client terminal; and
emulating said stored-value card responses in an interaction with said security module to receive responses from said security module, whereby network traffic between said load server and said client terminal is reduced.
19. A method according to any of claims 16 to 18, wherein said confirmation step includes the sub-steps of:

comparing said received stored-value card signature with an expected signature; and sending a confirmation message destined for said bank server, whereby said bank server is assured that said stored-value card has been loaded.
20. A computer-implemented method of interacting with a stored-value card by a client terminal to facilitate the loading of said stored-value card over a network, said method comprising the steps of:
receiving a load value from a bank server connected to said network;
emulating a plurality of security module commands that are sent to said stored-value card associated with said client terminal;
receiving a plurality of responses to said security module commands from said stored-value card;
grouping said responses to said security module commands from said stored-value card to form a load request; and
sending said load request to a load server over said network so that said load request may be processed by a security module associated with said load server to facilitate the loading of said stored-value

card over said network, whereby network traffic between said load server and said client terminal is reduced.
21. A method according to claim 20, wherein said network is an internet over which said recited steps of said methodoccur, wherein said bank server includes a bank web site for accepting a load request, and wherein said client terminal and said bank server are at separate locations.
22. A method according to claim 20 or 21, further comprising the steps of:
receiving an encrypted confirmation message from said load server that is unreadable by said client terminal; and
sending said encrypted confirmation message to said bank server, whereby said bank server is assured that said stored-value card has been

loaded.
23. A computer-implemented method of interacting with a security module by a load server to facilitate the loading of a stored-value card over a network, said method comprising the steps of:
receiving a load request from a client terminal over a network, said load request including a plurality of responses from a stored-value card generated in response to emulation of security module commands, whereby network traffic between said load server and said client terminal is reduced;
emulating said stored-value card responses in an interaction with said security module associated with said load server;
receiving a plurality of security module responses from said security module in response to said emulation; and
sending a load command destined to said client terminal over said network to facilitate loading of said stored-value card.
24. A method according to claim 23, wherein said network is an internet over which said recited steps of said method occur, and wherein said client terminal and said load server are at separate locations.
25. A method according to claim 23 or 24, further comprising the step of:

a confirmation step for performing the function of confirming loading of said stored-value card, whereby said bank server is assured that said stored-value card has been loaded.

...SPECIFICATION may wish to access any of a variety of Web servers in order to redeem **frequent flyer miles** , award points, etc., that he or she has **accumulated** . In this embodiment, a consumer has accumulated "points" through any of a variety of programs with airlines, restaurants, rental car companies, hotels, banks, **credit** or debit card issuers, telephone or other communication **company** , etc. The consumer wishes to redeem these points to receive free airline tickets, meals, car...

5/9,K/10 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01008315
INTERNET PAYMENT AND LOADING SYSTEM USING SMART CARD
CHIPKARTEN VERWENDENDES SYSTEM ZUM BEZAHLEN UND LADEN IM INTERNET
SYSTEME DE PAIEMENT ET DE CHARGEMENT PAR INTERNET A L'AIDE D'UNE CARTE A **PUCE**
PATENT ASSIGNEE:
VISA INTERNATIONAL SERVICE ASSOCIATION, (560813), 900 Metro Center Boulevard, Foster City, CA 94404, (US), (Proprietor designated states: all)

INVENTOR:
DAVIS, Virgil, M., 1121 Runnymead Drive, Los Altos, CA 94024, (US)
CUTINO, Suzanne, C., 431 Arkansas Street, San Francisco, CA 94107, (US)
BERG, Michael, J., 2644 Belmont Canyon Road, Belmont, CA 940002, (US)
CONKLIN, Fredrick, Sidney, 26 Alida Court, Oakland, CA 94602, (US)
PRINGLE, Steven, John, 5174 Miles Avenue, Oakland, CA 94618, (US)
LEGAL REPRESENTATIVE:
Finnie, Peter John et al (79521), Gill Jennings & Every, Broadgate House, 7 Eldon Street, London EC2M 7LH, (GB)
PATENT (CC, No, Kind, Date): EP 1023705 A1 000802 (Basic)
EP 1023705 B1 050406
WO 1998049658 981105
APPLICATION (CC, No, Date): EP 98920079 980430; WO 98US8806 980430
PRIORITY (CC, No, Date): US 45883 P 970430; US 951614 971016
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
RELATED DIVISIONAL NUMBER(S) - PN (AN):
EP 1003139 (EP 2000200558)
INTERNATIONAL PATENT CLASS (V7): G07F-019/00; G07F-007/10
CITED PATENTS (EP B): WO -96/04618 A; WO -96/13791 A; WO -96/32701 A
CITED PATENTS (WO A): WO 9632701 A ; WO 9604618 A ; WO 9613791 A
NOTE:
No A-document published by EPO
LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 000802 A1 Published application with search report
Application: 990407 A1 International application (Art. 158(1))
Lapse: 051228 B1 Date of lapse of European Patent in a contracting state (Country, date): SE
20050706, FI 20050406,
Grant: 050406 B1 Granted patent
Change: 001227 A1 Legal representative(s) changed 20001109
Examination: 000802 A1 Date of request for examination: 19991027
Examination: 001011 A1 Date of dispatch of the first examination report: 20000824
Change: 020703 A1 Legal representative(s) changed 20020516
Lapse: 051214 B1 Date of lapse of European Patent in a contracting state (Country, date): SE
20050706,
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count
CLAIMS B (English) 200514 972
CLAIMS B (German) 200514 903
CLAIMS B (French) 200514 1166
SPEC B (English) 200514 19407
Total word count - document A 0
Total word count - document B 22448
Total word count - documents A + B 22448

SPECIFICATION EP 1023705 B1

FIELD OF THE INVENTION

The present invention relates generally to a payment system and a value loading system using a computer network. More specifically, the present invention relates to a payment system and a value loading system for a smart card using an open network such as the Internet.

BACKGROUND OF THE INVENTION

With the explosive growth in open networks (such as the Internet) over the past several years and the rapid increase in the number of consumers

with access to the World Wide Web, there has been a great deal of interest in the development of electronic commerce on the Internet. Traditional financial transactions are being transformed.
A variety of service providers have introduced payment schemes to support the purchase of goods or services on-line in a virtual merchant environment. These approaches have used several models based on traditional payment methods existing in the face-to-face retail market, including credit/debit cards, checks and cash. However, for a variety of reasons, various of these numerous schemes have particular drawbacks.
Currently, a consumer may use his or her traditional credit or debit card to make a purchase over the Internet. A consumer simply supplies his card account number which is then transmitted across the Internet to a merchant and the payment transaction is completed in the traditional manner for a credit card. Often, these account numbers are transmitted over the Internet with extremely limited or no security. Security can be improved through use of the "Secure Electronic Transaction" protocol published by Visa International and Mastercard in 1996. These transactions still require some form of card validation and performance of a balance check. These checks are performed on-line between the merchant, an acquirer and an issuing bank, a process which can become time consuming and inefficient when the value of the transaction is low, or when a number of small value transactions will be taking place in a short time span.
The electronic check is modeled on the paper check, but is initiated electronically using digital signature and public cryptography. Deposits are gathered by banks via electronic mail and cleared through existing channels such as the Automated Clearing House (ACH). However, use of such an electronic check by a consumer has various drawbacks. For one, digital signatures and public encryption necessitate use of a certifying authority adding additional entities and "net" trips to the transaction. Also, cardholder registration is needed.
Other Internet payment alternatives are modeled on cash transactions and include a variety of schemes. With CyberCash, the consumer appends his credit card number to an electronic invoice received from the merchant, returns the credit card number to the merchant which is then processed and forwarded on to CyberCash where it is then treated like a normal credit card transaction. However, this technique suffers from some of the disadvantages discussed above with respect to traditional credit card transaction on the Internet and requires additional work by the merchant in processing the credit card number. Debit transactions may also be completed but require a consumer to open a CyberCash account in advance.
A digital, token-based system for Internet transactions has been implemented by DigiCash. With DigiCash, so-called "digital coins" are purchased from DigiCash from a prefunded deposit account and stored on the consumer's hard drive. These digital coins are then used for an Internet transaction with a merchant. This scheme has disadvantages in that the consumer must first set up a relationship with DigiCash and use a credit card or similar instrument to purchase these digital coins, which then must be downloaded to the consumer's computer. This transaction can be time consuming for the consumer and is subject to fraud. In addition, a merchant must be set up to not only accept these digital coins, but also to verify their authenticity, to confirm the transaction, and then finally to forward these numbers on to his bank in order to finally get paid. One drawback from the merchant's point of view is that much of the transaction work must be performed by the merchant.
Another scheme for completing an Internet transaction is offered by First Virtual Holding, Inc. First Virtual offers a software solution based upon a unique identification number and electronic mail confirmation. To use this scheme, a consumer opens a special account with

First Virtual and then receives a confidential identification number. When the consumer wishes to purchase a product or service over the Internet, he or she sends an electronic mail message containing the confidential identification number to the merchant. The merchant then sends the number to First Virtual by electronic mail for verification and identification of the customer. First Virtual then confirms with the consumer by electronic mail that the consumer did indeed initiate the transaction and wishes to make the purchase. There are drawbacks to this scheme in that the consumer must first open a special account with First Virtual. Also, the merchant must communicate with First Virtual to identify the customer and to identify the customer's credit card account number that is identified by the confidential identification number. Aside from payment schemes over the Internet, a technique in use for

performing a financial transaction at a stand-alone terminal uses a smart card. A smart card is typically a credit card-sized plastic card that includes a semiconductor chip for holding the digital equivalent of cash directly, instead of pointing to an account or providing credits. When a card of this kind is used to make a purchase, the digital equivalent of cash is transferred to the merchant's "cash register" and then to a financial institution. Stored-value cards are either replenishable (value can be reloaded onto the card using a terminal) or non-replenishable (the card is decremented in value for each transaction and thrown away when all its value is gone).

Physically, a smart card often resembles a traditional "credit" card having one or more semiconductor devices attached to a module embedded in the card, providing contacts to the outside world. The card can interface with a point-of-sale terminal, an ATM, or a card reader integrated into a telephone, a computer, a vending machine, or any other appliance. A microcontroller semiconductor device embedded in "processor" smart card allows the card to undertake a range of computational operations, protected storage, encryption and decision making. Such a microcontroller typically includes a microprocessor, memory, and other functional hardware elements. Various types of cards are described in "The Advanced Card Report: Smart Card Primer", Kenneth R. Ayer and Joseph F. Schuler, The Schuler Consultancy, 1993.

One example of a smart card implemented as a processor card is illustrated in FIG. 1. Of course, a smart card may be implemented in many ways, and need not necessarily include a microprocessor or other features. The smart card may be programmed with various types of functionality, such as a stored-value application: credit/debit; loyalty programs, etc. For the purpose of this disclosure, card 5 is programmed at least with a stored-value application, and will be referred to as "stored-value" card 5.

Stored-value card 5 has an embedded microcontroller 10 that includes a microprocessor 12, random access memory (RAM) 14, read-only memory (ROM) 16, non-volatile memory 18, an encryption module 22, and a card reader interface 24. Other features of the microcontroller may be present but are not shown, such as a clock, a random number generator, interrupt control, control logic, a charge pump, power connections, and interface contacts that allow the card to communicate with the outside world. Microprocessor 12 is any suitable central processing unit for executing commands and controlling the device. RAM 14 serves as storage for calculated results and as stack memory. ROM 16 stores the operating system, fixed data, standard routines, and look up tables. Non-volatile memory 18 (such as EPROM or EEPROM) serves to store information that must not be lost when the card is disconnected from a power source but that must also be alterable to accommodate data specific to individual cards or any changes possible over the card lifetime. This information might include a card identification number, a personal identification number,

authorization levels, cash balances, credit limits, etc. Encryption module 22 is an optional hardware module used for performing a variety of encryption algorithms. Card reader interface 24 includes the software and hardware necessary for communication with the outside world. A wide variety of interfaces are possible. By way of example, interface 24 may provide a contact interface, a close-coupled interface, a remote-coupled interface, or a variety of other interfaces. With a contact interface, signals from the microcontroller are routed to a number of metal contacts on the outside of the card which come in physical contact with similar contacts of a card reader device.

One possible use of a stored-value card by a consumer is illustrated in FIG. 2. FIG. 2 illustrates a block diagram of a customer operated service payment terminal 50. A customer typically uses such a service payment terminal in a face-to-face environment in order to purchase goods in a store or directly from the terminal itself. Service payment terminal 50 can be an attended device or it can be integrated into a self-service device such as a vending machine or public telephone. For example, the service payment terminal may be incorporated into a soda machine in order to dispense sodas to a customer in which the customer pays by inserting the stored-value card. Or, the service payment terminal may be a point-of-sale terminal such as is found at a check-out counter where a customer inserts his stored-value card in order to purchase goods. Service payment terminal 50 includes a router 51, a user interface 52, a card handler/reader 54, a security card handler 56, a security card 58, a terminal application 60, a data store 64 and a concentration point handler 66. Router 51 is hardware and software for routing information between functional blocks. User interface 52 controls the status of displays on the terminal and supplies instructions to the user. For example, the user interface provides instructions relating to insertion of stored-value card 5 or security card 58. Also, the user interface provides instructions and/or buttons for the customer to interact with terminal application 60 in order to purchase goods and/or services. Card handler 54 provides a physical card reader and associated software for accepting and communicating with stored-value card 5. Similarly, security card handler 56 provides a card reader and associated software for communicating with security card 58. In conjunction with security card handler 56, security card 58 controls the command sequence of the terminal and provides transaction and a batch security.

Terminal application 60 receives commands and information about the transaction and initiates the actual purchase. In addition, terminal application 60 is responsible for all application specific functionality such as guiding the customer through the use of the terminal via a display, and for providing all hardware and software needed to provide the user with a good and/or service once it has been informed by the security card that an appropriate value has been deducted from the stored-value card.

Data store 64 controls the storage of purchase transactions and totals. Concentration point handler 66 controls the sending and receiving of information to and from a concentration point. Concentration point 68 is a staging computer that communicates with any number of service payment terminals to collect batches of transactions. The concentration point then sends these transaction batches to a clearing and administration system for processing (such as in FIG. 3). Once processed, batch acknowledgments, along with other system updates are sent to the terminals via the concentration point. The concentration point ensures a successful transfer of data between service payment terminals and the clearing and administration system, and prevents overloading of the clearing and administration system. The service provider contracts with a concentration point for collection of the service payments. The concentration point may also be an existing central facility such as a

telephone company that collects its own payments from card telephones. Such a service payment terminal 50 allows a customer to use a stored-value card for the payment of goods and/or services, generates a payment result from a transaction, and bundles individual payment results into a collection for transfer to a clearing and administration system, which then transfers funds that had been debited from a customer's stored-value card to the merchant whose goods and/or services had been purchased from the terminal.

FIG. 3 illustrates an environment 100 useful for issuing stored-value cards and reconciling transactions performed with such a card. A terminal supplier 102 builds the equipment used by a service provider 104 to provide goods and/or services to customers having a stored-value card at a service payment terminal 50. Card Supplier 106 contracts with an integrated circuit manufacturer and a card manufacturer for integrated circuits and plastic card bodies, then embeds the integrated circuits into the cards and initializes them with a serial number. It then delivers the cards to card issuer 108. In conjunction with clearing and administration system 110 (such as a system provided by Visa International of Foster City, CA), card issuer 108 personalizes new cards and then transfers these cards to individuals (cardholders 112). The cardholder may then charge the card with value prior to use. Alternatively, the card may come with value already loaded. The cardholder 112 may then use the card at a service payment terminal 50 to purchase goods and/or services from service provider 104. Terminal 50 then debits the value from the card, thus creating a service payment. Periodically, all transactions are sent in a data file from terminal 50 via concentration point 68 and an acquirer 114 to clearing and batch administration system 110 along with accumulated service payment batches from other terminals. Based upon this collection data, clearing and administration system 110 then receives money from card issuer 108 which had originally come from cardholder 112. Clearing and administration system 110 then transfers a lump sum to acquirer 114 using a suitable settlement service (such as one provided by Visa International) to pay the various service providers having a relationship with acquirer 114. Based upon the previous collection data, acquirer 114 then transfers an appropriate amount of money to each service provider 104 reflecting the value of the goods and/or services that that service provider had provided that day to cardholders based upon deductions from their stored-value cards.

Although such a service payment terminal described above is useful for the on-site purchase of goods by a consumer with a smart card, it does not permit the purchase of goods and/or services by a customer over a network. Nor does such a terminal permit the immediate transfer of electronic information to a consumer's computer. Service payment terminals are typically specially-designed units of hardware and software

located at a merchant site. Furthermore, the service payment terminal is designed to integrate into one hardware location the functions of the terminal application (providing goods and/or services), a card handler for the stored-value card, and the transaction management embodied in the security card. Such a design is not suitable for transactions where a customer may wish to perform a transaction from almost any location (including the home or office) quickly and easily with a minimum of prearranged set-up and expense. Furthermore, although various Internet payment schemes have been suggested, they are not oriented toward small value transactions, and do not allow the use of a smart card for transactions over the Internet.

Thus, it would be desirable to have an architecture and system that would allow a consumer to quickly and easily perform transactions over an open network such as the Internet using a smart card. It is also

desirable to have an architecture and system in which a user may use a smart card for both purchases over the Internet as well as purchases at existing service payment terminals.
However, in order to purchase, the card must be loaded with value first. Value can be loaded onto a stored-value card in a variety of ways. Currently, it is inconvenient for a user to load value onto his or her stored-value card. A user must physically travel to a bank or other institution that has an automated teller machine (ATM) or other similar device in order to load value on to his or her stored-value card. The user can insert money into the machine and have a corresponding value put onto the stored-value car, the user can use a debit card to deduct value from the user's account at the bank for transfer to the card, or a credit card can be used as the source of funds to be transferred to the stored-value card. In either case the user must travel to the bank to load value. Further creating difficulty is that not all banks or other financial institutions have such a machine for loading value onto a user's stored-value card.
WO 96/04618 discloses a terminal for remote purchase payment and bill payment transactions. Data is exchanged with a remote server. Embodiments of WO 96/04618 have a smart card. The user inputs a cash amount to the terminal, the smart card is verified to check that there is sufficient credit on the card, and then a remote merchant terminal is accessed. A purchase log in the terminal is then updated.
WO 96/32701 describes a network of retailer server stations and customer stations. The retailer server generates a payment slip including various data items which is transmitted over the network to the payment server, which queries the customer account. If the payment server is authorised, the payment server generates a cash voucher which is transmitted to the retailer to allow the transaction to proceed.
Accordingly, it would also be desirable to have a technique to allow a user to conveniently and easily load value onto a stored-value card.

Summary of the Invention
To achieve the foregoing, and in accordance with the purposes of the present invention, an architecture and system is disclosed that enables the use of a smart card for payment of goods and/or services purchased on-line over an opennetwork such as the Internet. Further, an architecture and system is disclosed that enables a smart card to be loaded with value on-line over an open network such as the Internet.
In a first aspect, the present invention provides an electronic commerce payment solution offering consumers an on-line equivalent to purchases with cash or coins. It extends the notion of a smart card to the Internet marketplace, providing an alternative for low-value transactions. The present invention facilitates not only the purchase of physical goods, but also the purchase of digital merchandise (such as electronic information).
In one embodiment of the present invention, a client server on a client terminal controls the interaction with the consumer and interfaces to a card reader which accepts the consumer's smart card, which, in one specific embodiment, includes a stored-value application. For the purposes of this description, the smart card with a stored-value application used in embodiments of the invention will be simply referred to as a "stored-value card." A payment server on the Internet includes a computer and terminals that contain security cards to handle the transaction, data store and collection. Also connected to the client terminal and the payment server over the Internet is a merchant server advertising the goods and/or services offered by a merchant for sale. In one embodiment of the invention, the merchant server includes a web site and the merchant has contracted with an acquirer to accept stored-value card payments for goods and/or services purchased over the Internet.

Thus, a consumer may use his or her stored-value card at a client terminal location in order to purchase goods and/or services from a remote merchant server. The Internet provides the routing functionality among the client terminal, merchant server and payment server.
From the consumer's perspective, the present invention operates in a similar fashion as using a stored-value card in a real merchant environment. The transaction process is similar to the interaction between a stored-value card and a service payment terminal in a face-to-face merchant environment, but with functionality distributed across the Internet between the card reading device located where the customer is, the merchant server advertising the merchant's wares, and a payment server with a security card that manages the transaction. All of these entities may be physically remote from one another with router functionality being provided by the Internet. The present invention is easy to use. A consumer need not establish a new relationship with a bank or other Internet service company, nor create a special Internet deposit account in order to begin purchasing goods and/or services on the Internet. A consumer simply makes use of currently available stored-value cards in order to make an Internet purchase.
When browsing merchant store fronts on the Internet and deciding to purchase goods and/or services, the cardholder selects the stored-value card payment option offered by the merchant. The cardholder then inserts his or her card into a card reader attached to a personal computer (for example). The cardholder's balance and purchase amount are displayed, the cardholder approves the purchase, and the amount is deducted from the value stored on the stored-value card. The transaction amount is captured by the security card or the merchant server for subsequent batch settlement through a clearing and administration system to the issuer and acquirer. In one embodiment, the transaction security and authentication for the system follows a similar methodology as that used in an actual service payment terminal between a stored-value card and the security card in the terminal. Advantageously, a customer may make use of pre-existing stored-value cards for purchases over the Internet without any prior arrangement of an account, purchases of credits or tokens, or establishment of a new relationship with a bank or other company.
In addition, once a value has been deducted from the stored-value card, the merchant has been informed, and the security card in the payment server has recorded the transaction, an existing clearing and administration system may be used to reconcile the transaction and to pay the appropriate parties. Advantageously, a new system and methodology for reconciling transactions need not be developed or implemented. A pre-existing clearing and administration system may be used which greatly simplifies implementation of the present invention.
Use of a stored-value card as payment for Internet transactions provides numerous advantages. For example, a stored-value card can be used in small transactions where credit cards or checks would be unrealistic. Other advantages to the consumer include enhancing the value of a stored-value card by enabling access to both real and Internet merchant environments with a single card. The present invention also allows an anonymous payment solution for transactions over open networks. Furthermore, in one embodiment of the invention the stored-value card is implemented on a traditional credit card; a single card thus provides payment solutions for both low and high value transactions.
In addition, use of a stored-value card is extremely advantageous for small dollar amount transactions. Often, consumers are reluctant to use, and merchants are reluctant to accept, credit card transactions for small dollar amounts. For the consumer and the merchant dealing with many of these small transactions can be a bookkeeping headache and may not be worth the expense. A merchant may also be unlikely to accept a credit card for a small dollar amount transaction because of the service fees

per transaction. By permitting the use of a stored-value card to make purchases over the Internet for small dollar amounts, a merchant may very well be able to begin charging for goods and/or services that he had been providing for free in the past. One embodiment of the invention works well with purchases of under $10.00. although purchases of any amount may be made.

The present invention also provides numerous advantages to merchants who wish to sell goods and/or services over the Internet. For example, the present invention provides a payment solution for low-value transactions, enabling merchants to offer a wider range of digital merchandise. A merchant is also provided a method to recover costs of services not previously charged for, and is provided immediate access to an existing, and rapidly growing, cardholder base. Furthermore, the present invention integrates into an existing clearing and administration system meaning that the merchant need not implement or become familiar with new procedures for reconciliation of transactions.

Furthermore, a merchant need only make a minimal investment in time and money to take advantage of the present invention and to accept payments over the Internet. The merchant need not engage in the development of

complex software or accounting procedures. Thus, smaller merchants will especially benefit from the present invention. By establishing a business relationship with an acquirer and incorporating standard merchant software, a merchant is ready to begin selling goods and/or services from his web site. Because a smart card with a stored-value application is used, the payment server and the client terminal perform the details of the transaction and a merchant is relieved from having to control and keep track of a transaction. Also, the payment server and its associated security cards manage and provide security for the transaction. From a merchant's point of view, the merchant knows that a consumer desires to purchase an item and that a cost has been transmitted to the consumer, thus, when the merchant receives a confirmation message, the merchant may release the item to the consumer. The merchant need not be concerned about security nor be responsible for authenticating a stored-value card nor for determining a balance on the card. Of course, a payment server could coexist along with the merchant server or could even be the same computer. That is, a merchant could implement payment server functionality at its own site if it so desired.

In a second aspect of the present invention, a loading technique allows the consumer to conveniently load value on to his or her stored-value card from any suitable device via an open network such as the Internet. A consumer is allowed to use any suitable computer at the home, office or elsewhere in order to connect to his bank or other financial institution. Using appropriate message integrity, value is transferred from the bank to the consumer's stored-value card. At the same time, the corresponding value is transferred from the bank to the stored-value card issuer through existing networks for later settlement with a merchant from whom the consumer purchases goods or services. Advantageously, this embodiment makes use of an existing clearing and administration system for eventual settlement of the transaction between the merchant and the card issuer. Also, the transaction is fully auditable and a log of previous transactions is stored on the card for later display. Thus, a consumer may conveniently load value on to his or her card while a high level of security is maintained and the card issuer can take advantage of unspent funds on the card.

From the consumer's perspective, the present invention operates in a fashion similar to loading a stored-value card at an ATM machine, except that the consumer need not insert cash or an additional debit or credit card, nor need travel to a bank. The loading functionality is distributed across the Internet between the card reading device located where the

customer is, a bank server holding the consumer's account, and a load server with a host security module that provides security. All of these entities may be physically remote from one another with router functionality being provided by the Internet.

Furthermore, a bank need only make a minimal investment in time and money to take advantage of the present invention in order to allow its customers to load value from their existing accounts over the Internet. The bank need not engage in the development of complex custom software or accounting procedures. By incorporating software libraries, a bank is ready to begin loading value onto its customer's cards from its web site. Preferably, libraries are provided that interface with an existing server at a bank to facilitate the building of an HTML page. Because a smart card with a stored-value application is used, the bank server, load server and client terminal perform the details of the transaction and the bank itself is relieved from having to control and keep track of a transaction. Also, the load server and stored-value card manage and provide security for the transaction. I.e., the bank need not be concerned about security nor be responsible for authenticating a stored-value card nor for determining a balance on the card. Of course, a load server could coexist alongside the bank server or could even be the same computer. That is, a bank could implement load server functionality at its own site if it so desired. In a preferred embodiment, the load server and its security module is provided by a separate financial institution or by a third-party processor.

Both of the payment and loading aspects of the present invention provide benefits to issuers and acquirers. Expansion of the functionality for a stored-value card increases revenue opportunities from cardholders and merchants. Also, there may be new merchant marketing opportunities for acquirers. The present invention also offers a micro-payment solution for electronic commerce without the need to introduce a separate product or brand or to establish new service provider relationships. In addition, in one specific embodiment of the invention, funds that are loaded onto a card are transferred from the loading bank to the card issuer so that the issuer may take advantage of the funds on the card until they are spent.

A further advantage of both aspects of the present invention is its ability to minimize transaction traffic on the Intemet and to minimize the amount of time that a security card (or a security module) is tied up with one transaction. In the payment aspect, by emulating security card commands issued to a stored-value card, a client terminal is able to receive and group responses for transmission to a payment server all at once, rather than one-by-one over the Internet. The payment server is then able to emulate a stored-value card as it interacts with the security card in delivering the responses to the security card. The result is less message traffic over the Internet, saving time and interrupts.

Also, by delivering an expected stored-value card signature to the payment server, the security card is relieved from having to compare the signatures itself, and may release sooner and move on to a new transaction. The payment server may also deliver the expected stored-value card signature to the client terminal or merchant server for comparison, thus reducing to one round trip the message traffic between the payment server and the client terminal.

The present invention is suitable for use with any type of stored-value card that is able to store an amount and to decrement a value upon a command. In one embodiment of the invention, a stored-value card implemented as a processor card works well. Use of a processor card has advantages where information processing is done on the card rather than in the terminal or host computer. Processor cards allow encryption to be done by the card, allow generation of signatures, and can accommodate multiple passwords or personal identification (such as biometrics that

uniquely identify the holder of the card). Processor cards also provide increased data security, an anti-fraud capability, flexibility in applications, a multi-purpose capability, and off-line validation. Because high telecommunication costs and/or low reliability of a network may make on-line authorization impractical, a stored-value card with the capability for performing off-line processing and authentication by itself is extremely valuable.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention, together with further advantages thereof, may best be understood by reference to the following description taken in conjunction with the accompanying drawings in which:

FIG. 1 is a block diagram of an example of a stored-value card useful in embodiments of the present invention.

FIG. 2 is a block diagram of a service payment terminal in which a stored-value card may be inserted to purchase merchandise.

FIG. 3 is a block diagram of an example of a clearing and administration system useful for reconciling financial transactions received from a service payment terminal.

FIG. 4 illustrates an architecture and system for payment over the Internet using a stored-value card.

FIG. 5 illustrates a payment embodiment of the present invention.

FIG. 6 illustrates another payment embodiment of the present invention in which the security card releases earlier.

FIG. 7 illustrates yet another payment embodiment of the present invention having fewer round trip messages between the client terminal and payment server.

FIG. 8 illustrates still another payment embodiment of the present invention in which the merchant server compares stored-value card signatures.

FIG. 9 illustrates an added encryption layer useful for embodiments of the present invention.

FIG. 10 is a flowchart describing a user's perspective of a stored-value card purchase transaction using the present invention.

FIGS. 11A-11D are a flowchart describing the processing of a user purchase using an embodiment of the present invention.

FIG. 12 is a flowchart describing the alternative embodiment of FIG. 6.

FIG. 13 is a flowchart describing the alternative embodiment of FIG. 7.

FIG. 14 is a flowchart describing the alternative embodiment of FIG. 8.

FIGS. 15A and 15B are a flowchart describing the added security layer of FIG. 9.

FIG. 16 illustrates an architecture and system for authentication over an internet using a stored-value card.

FIG. 17 illustrates a system for loading value onto a stored-value card according to one embodiment of the present invention.

FIGS. 18A-18D are a flowchart describing the loading of a consumer's stored-value card using an embodiment of the present invention.

FIG. 19 is a block diagram of a typical computer system suitable for use in embodiments of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

GENERAL ARCHITECTURE

The present invention separates the functionality involved in a transaction using a stored-value card in order to take advantage of the routing capabilities of the Internet. FIG. 4 illustrates symbolically an architecture 200 for an internet payment system involving a smart card,

such as a smart card having a stored-value capability. An internet loading system is shown in FIG. 17 and may have similar functionality as described below. Shown is an internet 202, a client terminal 204, a

payment server 206 and a merchant server 208. Local cardholder functions including a consumer card interface, display and accept/cancel options are performed at client terminal 204. Payment functions including security card control, data store and use of a concentration point are performed by payment server 206. The presentation and eventual delivery of goods and/or services by a merchant are performed under control of merchant server 208. The internet 202 performs routing functions between each entity. It should be appreciated that internet 202 may take the form of the Internet currently in use, or may also be any other open network implemented using any combination of computer, telephone, microwave, satellite, and/or cable networks.

Basically, client terminal 204 controls the interaction with a user and interfaces to card reader 210 which accepts a smart card having a stored-value application. For simplicity, throughout the remainder of this specification, card 5 will be referred to as a stored-value card (SVC) 5. Payment server 206 communicates directly with a terminal or through a concentrator 212 that handles any number of terminals 214-216 each having a security card 218 and 220 respectively. Payment server 206 also communicates with concentration point 68 for transmission of transaction data to a clearing and administration system. Database 223 stores all suitable information passing through payment server 206 for each transaction. Use of such a database allows any number of merchants (or merchant servers) to use payment server 206 for transactions. Payment server 206 controls payment functions such as handling the attached terminals, managing data base 223 and collection functions. Merchant server 208 is a site that has contracted with an acquirer to accept stored-value card transactions as payments for goods and/or services purchased over the Internet.

Stored-value card 5 may take a variety of forms and is useful in many situations where it is desirable to store monetary value on a card that a consumer may use. In general, a stored-value card is any card or similar device that is able to store a value that is decremented when the card is used. The card may be purchased complete with a stored-value or value may be later added to the card by a user. Such cards may also have their value replenished. Of course, a stored-value card need not be in the form of the traditional credit card, but could appear in any form and of any material that is able to store value and be manipulated by a user for a payment transaction. By way of example, other forms that a stored-value card may take are any electronic representations. Further, the functionality of stored-value card 5 may be implemented in software on client terminal 204, that is, card 5 may be a "virtual" card.

A stored-value card may also perform a variety of functions in addition to simply storing value. A card may be dedicated to the storing value or may contain memory and programs for other applications as well. By way of example, an "electronic wallet" refers to a processor card that can execute a variety of financial transactions and identification functions. Such a card may serve debit, credit, prepayment, and other functions. A stored-value card typically includes information such as a bank identifier number, a sequence number, a purchase key, a load key, an update key, an expiration date, a transaction counter, a session key, etc., in addition to a running balance.

A stored-value card may also be termed a prepayment card, a cash card, or a decrement-in-value card. A stored-value card may also be implemented by using a variety of card technologies. By way of example, a stored-value card is typically implemented as a card containing one or more integrated circuits. One example of an integrated circuit card is a

memory card that has a semiconductor device for storing information but lacks calculating capability. Another example of an integrated circuit card is a processor card that has not only memory but also a microcontroller to enable the card to make decision. A processor card may also be termed a microprocessor card or a "smart card".
A processor card may include an encryption module in order to provide a variety of security precautions. By way of example, security precautions may include simple PIN numbers, biometrics, simple algorithms, or sophisticated algorithms such as the Data Encryption Standard (DES) or Rivest, Shamir, Adelman (RSA) encryption. The card is thus able to use these precautions to verify users, card readers, etc., to validate security cards and/or to provide a unique signature. Preferably card 5 includes any number of keys known to the card issuer that are used during the course of a payment or load transaction to generate signatures for validation of the stored-value card, validation of the security card or module, and validation of the system itself.
Client terminal 204 is any suitable device for interacting with a stored-valued card 5 and for communicating over a network to a payment server or a merchant server. By way of example, client terminal 204 may be a mainframe computer, a work station, a personal computer, a kiosk, or any type of service payment terminal that a consumer might use to purchase goods and/or services. Furthermore, client terminal 204 may also be embodied in any portable device such as a laptop computer, a cellular telephone, or any variety of a personal digital assistant (PDA) such as those made by Apple Computer, Inc. or by U.S. Robotics. Card reader 210 is any suitable interface device that functions to transfer information and commands between client terminal 204 and stored-value card 5. By way of example, card reader 210 may be a card reader manufactured by Fischer-Farr International of Naples, Florida, by Hewlett-Packard of Palo Alto, California, by Schlumberger, by Gem Plus, etc. Card reader 210 may take any variety of forms such as a stand alone unit, integrated with the client terminal, attached to the keyboard of the client terminal, or even built in to a floppy disk-sized unit capable of being read from a disk drive of the client terminal, etc.
Client terminal 204 includes client code module 224 and card reader module 226. Reader module 226 may be implemented using any suitable software and libraries for communicating with card reader 210 and its actual implementation will depend upon the type of card reader used. Client module 224 controls communication between the client terminal, the card reader, the payment server and the merchant server. Client module 224 may be implemented using any suitable code. In one embodiment of the invention, client module 224 is implemented using a combination of "C" code and a Java applet. The applet is also supplemented with parameters from an HTML page sent from the merchant server. It is contemplated that Java code works well for implementing the modules on the client, payment and merchant servers because it is platform independent, and could even replace the "C" and "C++" code used.
Client module 224 is also responsible for controlling displays to the user and for the interaction between the card and the card reader. The module also builds the draw request message after receiving all of the start-up information from the card and the amount of the purchase from the merchant server. The client module is able to communicate with all components on the Internet, either directly or indirectly.
Payment server 206 includes payment code module 228 and terminal interface 230. As with client terminal 204, payment server 206 may be implemented using any suitable computer. By way of example, a personal computer works well. There may be one payment server for each merchant server or a single payment server may service any number of merchant servers. Alternatively, there may be multiple payment servers for a single merchant. In addition, payment server 206 need not be remote from

merchant server 208 but may be located at the same site and have a different Internet address, or the payment server and the merchant server may even be implemented on the same computer. Payment server 206 is designed to facilitate the communication between the user's stored-value card and a terminal's security card. If a part of a transaction fails to complete, the payment server may notify the participating system components.

Payment module 228 may be implemented using any suitable code. By way of example, payment module 228 is implemented using a combination of "C" code, "C++" code and Java code. Payment module 228 is, in one specific

embodiment, a multi-threaded process that can service multiple concurrent client applet transactions on demand. The module is responsible for controlling all interactions with the terminals and their concentrator including the transaction collection function. For individual transactions, the payment module controls the message flows and logs interim results. When an applet connects with the payment server, it creates a transaction thread to support the transaction through its life cycle. Each thread, in turn, assigns a terminal for communication. Having a one-to-one correspondence between transaction threads and terminals has been found to provide desirable results.

Terminal interface 230 is any suitable set of software and libraries for communicating with a terminal 214 either directly or, as shown, through terminal concentrator 212. The actual implementation of terminal interface 230 will depend upon the type of terminal used. A terminal such as 214 may be any suitable terminal such as are known in the art. By way of example, an iq Delta 2010 terminal made by Schlumberger has been found to provide desirable results. Such a terminal may support a variety of commands originating from the terminal interface. These commands emulate the normal responses that an attached terminal would pass from the stored-value card to the security card. The actual security card commands are held in the terminal while the terminal performs the tasks necessary to simulate the presence of a stored-value card.

Security card 218 may be any suitable security card such as are known in the art (often referred to as a Purchase Secure Application Module--PSAM). In other embodiments, the functionality of security card 218 can be replaced by a hardware security module, could be implemented in hardware within the payment server, or could even be implemented in

software.

By way of example, security card 218 is a removable credit card-sized processor card that is programmed to process and store data relating to financial transactions. Security card 218 contains a microchip embedded in the card that enables the security card to authenticate and to validate the user's stored-value card. If a user stored-value card is accepted by the security card, and the stored-value card contains sufficient value, the security card guarantees that the merchant providing the goods and/or services receives payment according to the amount deducted from the stored-value card for the goods and/or services rendered. In a preferred embodiment, the security card also contains DES purchase security keys and authenticates the stored-value card during a purchase transaction and secures the payment and collection totals. A security card also stores signature algorithms for stored-value cards in use. A security card may also contain a transaction identifier for the current transaction, a financial sum of all transactions remaining to be settled, a session key, and master keys for all stored-value cards in use. Further, the security card may contain generations of keys, blocked card indicators, date of last update, multiple card programs, different currency rates and additional security.

Concentration point 68 is a staging computer that communicates with

terminals to collect batches of purchase transactions. The concentration point then sends these transaction batches to a clearing and administration system for processing. Once processed, batch acknowledgments, along with other system updates, are sent back to the terminals via the concentration point.

Merchant server 208 includes a merchant code module 232. Merchant server 208 may be implemented upon any suitable computer capable of communicating with and presenting information to users over an internet. Merchant code module 232 may be implemented using any suitable code. By way of example, merchant module 232 may be implemented using a combination of Perl, HTML, and Java code. Merchant server 208 is typically a generic web server customized for the merchant's business. Merchant server 208 may include databases, CGI scripts and back-office programs that produce HTML pages for an Internet user.

A brief discussion of the flow of a transaction now follows. During a financial transaction, the client terminal and merchant server exchange information 234 via internet 202. Each transaction initiated by a user has a transaction identifier created at the merchant server, and a merchant identifier unique to the payment server is also available from the merchant server. Client module 224 and the payment server also use this unique transaction identifier for tracking and logging information about the transaction. Merchant server 208 generates a unique identification of the transaction, completes other required parameters, encrypts as appropriate, and builds an HTML page and sends it to the client terminal. The client module interacts 235 with the stored-value card and builds a draw request message containing related card information, the purchase amount, and other information supplied by the merchant server.

The client terminal then communicates 236 with payment server 206, first by forwarding the draw request to the payment server. Payment server 206 verifies the transaction to determine if it is a valid transaction from a known merchant. The transaction is logged into the payment server's transaction database 223. Upon completion of a transaction, payment server 206 builds a result message containing the identification of the transaction and signs it. The message is then routed to merchant server 208 via client terminal 204. Merchant server 208 then validates the result message. After determining that the transaction was successful, merchant server 208 creates an HTML page for the purchased information and sends it to client terminal 204. Alternatively, the merchant may also deliver purchased goods to the user at this point. It is also possible for the payment server and the merchant server to communicate information 238 directly between themselves. Preferably, as client terminal 204 has already established communication with the merchant server and the payment server, links 234 and 236 are used to exchange information between the payment server and the merchant server, rather than establishing a new link 238.

USER PERSPECTIVE OF A PAYMENT TRANSACTION

FIG. 10 is a flowchart describing an embodiment of the present invention from a user's perspective such as may occur with the embodiment of the invention shown in FIG. 4. In step 502, a user acquires and adds value to a stored-value card. Alternatively, a user may acquire a stored-value card that already contains value. This stored-value card may take the form of any of the above-described stored-value cards that are able to store value and to debit value from the card. In step 504 the user accesses the merchant server web site via communication link 234 over the Internet. This access of a web site may be performed in any suitable fashion such as by using any commercially available web browser. In step 506 the user inserts a stored-value card in card reader 210 at the user's terminal. Alternatively, the user may insert the card before

accessing the web site, or even after the selection of goods and/or services from the merchant web site. In step 508 the user browses the merchant web site and selects goods and/or services for purchase from the merchant using the web site interface that the merchant has provided. The user then selects an appropriate button on the merchant web site to indicate what the user wishes to purchase. Next, in step 510 the user receives a total sale amount from the merchant server and is directed to actuate a button on the web site indicating that the user wishes to proceed with the purchase using the stored-value card.

In step 512 the architecture and system of the present invention (such as is shown in FIG. 4, for example) processes the user order by way of the payment server, terminal and security card. In step 514, the user's stored-value card is debited by the total sale amount and the user receives a "debited" message at the user's terminal. This message is optional if the system is designed so as to not inform the user of this debit. In step 516 the user receives a confirmation message from the merchant server indicating that the transaction has been completed. The user may now download the purchased information and/or receive a receipt for goods and/or services to be rendered or delivered from the merchant at a later date. In step 518 the merchant, via a clearing and administration system, receives payment to its bank account for the goods and/or services rendered by way of information collected from the payment server. In one embodiment of the invention, an existing clearing and administration system is used, as well as an existing methodology for transferring information from a security card for later reconciliation. This use of an existing "back end" allows systems of the invention to be implemented quickly and cheaply. This approach also ensures that cards used in the system are compatible with other stored-value terminals.

DETAILED PAYMENT TRANSACTION FLOW

FIG. 5 illustrates a detailed embodiment of internet payment architecture 200 having client terminal 204, payment server 206 and merchant server 208. A stored-value card 5 is in communication with client terminal 204, and a security card 218 inside a terminal 214 is in communication with payment server 206. Not shown for simplicity in this figure are other elements of the system shown in FIG. 4. One embodiment of a technique by which a financial transaction may be completed over the Internet will now be described using the flowchart of FIGS. 11A through 11D with reference to FIG. 5.

It should be appreciated that a wide variety of terminology may be used to describe message flow throughout the architecture. For example, the terminology used herein to describe the sequential messages draw request, debit, success, and confirmation, may also be referred to by the respective terminology: draw request, debit IEP, debit response, and debit result (or message result).

Initially, a suitable web browser of client terminal 204 is used by the user to access a merchant server web site as indicated by 302. In step 602, the user selects goods and/or services from the merchant site and indicates to the site that the user wishes to purchase these items using a stored-value card as indicated at 304. In step 604 the merchant server receives this request for a stored-value card transaction.

In step 606 the merchant server builds an HTML page that includes the following client applet parameters: the total cost of the transaction as determined by the merchant server; the type of currency being used; the port and IP address of the payment server; a unique transaction identifier used by both the payment server and the merchant server to track a transaction; and a unique merchant identifier assigned to the merchant by the acquirer and known to the payment server. Other information may also be included such as the currency's exponent, a status URL address of the merchant server used for communication from the

client terminal, and a merchant server generated key and other security information to ensure the identity of the merchant server and the integrity of the message. Other process related information such as software release level, encryption methodology and keys may also be conveyed. Once this page has been built, the page is sent 306 to the requesting client browser and triggers the loading of the client code module (in this example a Java applet) in the client terminal.

Some browsers may not allow an applet to invoke a dynamic link library (DLL) due to security reasons. In an embodiment of the present invention, the client applet along with any DLLs needed are preloaded on the client terminal. Then, the merchant server is allowed to invoke the client applet and DLLs dynamically to circumvent this security precaution.
In step 608 the client module of the client terminal interacts with stored-value card 5 to obtain card information 308 in order to build a draw request message for later transmission 310 to payment server 206. In one embodiment of the invention, the client applet loads a local DLL, makes an API call to that library, which in turn makes a call to another DLL that finally makes a call to the card reader. In this fashion communication with the card is achieved. Once responses from the card are received, the client module will also combine these responses into a byte stream suitable for transmission over a network to a payment server. Also at this point, the currency type and expiration date on the card are checked, and the total cost of the ordered merchandise is checked against the card balance to ensure that the value on the card is great enough to cover the transaction. If the checks are not successful, a message to that effect is delivered to the user and this transaction terminates.
The client module emulates a variety of security card commands to receive responses from these commands from the stored-value card. Because the stored-value card and the security card are now physically separated from one another, and communication takes place over the Internet, it would not be advantageous to engage in numerous commands and responses over such an open network. In the interest of speed and reliability, it is advantageous to have fewer messages exchanged.
To operate securely and reliably in this environment, in one embodiment of the present invention, client module 224 emulates a security card and gathers all the responses for transmission in one draw request message. The draw request message may include a variety of information including a draw request token, state information, the merchant identifier, the transaction identifier, security information, a purse provider identifier, an intersector electronic purse (IEP) identifier, an algorithm used by the card, an expiry date, the balance of the card, a currency code, a currency exponent, the authentication mode of the IEP, the transaction number of the IEP, a key version and the purchase amount. As all of this information is prepackaged into a single draw request message, the number of messages between the stored-value card and the security card over the Internet is greatly reduced.
In this embodiment, the draw request message is built by packaging the stored-value card's response to the "reset" and "initialize" commands and any public key certificates along with the total cost and the currency of the transaction received from the HTML page. For public key cards, the card and issuer certificates are obtained from read commands and may also be included in the draw request. By packaging all of this information together into one draw request message, it is possible to cut down on the number of messages exchanged between the client server and the payment server, and reliability and speed is improved. In one embodiment of the invention, an intersector electronic purse (IEP) protocol is used to reset and initialize the card and to receive a response.
Next, in step 610 the client terminal accesses the payment server using the IP address received from the merchant server. In step 612 the client

terminal sends the draw request message to the payment server as indicated at 310. The client terminal also creates a log of this message being sent.

In step 614 the payment server processes the draw request in conjunction with an associated security card as will be explained in greater detail below with reference to FIG. 11D. Draw request 312 is shown being sent to terminal 214. In one embodiment of the invention, the payment server creates a transaction thread for each connected client module to service it through the life cycle of the transaction. After step 614, the payment server has received a debit command and a security card signature 314 from the security card in the terminal. This debit command may also be termed a "debit IEP" command. The security card signature is a value that uniquely identifies and validates security card 218 to prove to stored-value card 5 that the incoming debit command is a valid command from a real security card. This validation ensures that when the stored-value card is debited. that the financial totals in the security card are updated. Thus, the user of the stored-value card is guaranteed that a valid debit of the card has occurred. In a preferred embodiment of the invention, the security card signature is an encrypted value ensuring that no other entity can forge an identity of a security card.

In step 616 the payment server sends the debit command along with the security card signature to the client terminal as indicated at 316 for the stored-value card to debit itself. At this time, the payment server also logs this debit command into its database.

In step 618, upon receiving the debit command from the payment server, the client module replaces the amount in the debit command with the original amount (from the merchant server) to ensure that the amount has not been tampered with while traveling over the network. At this time, the client module also creates a log of the debit command. Client module 224 then passes 318 the debit command and security card signature to stored-value card 5 which verifies the signature, debits itself by the purchase amount, and also generates a success message (also termed a "debit response" message) and a stored-value card signature. The stored-value card signature is a unique value identifying a valid stored-value card. In a preferred embodiment of the invention, this signature is in encrypted form to prevent tampering. If card 5 does not have enough value to satisfy the purchase amount, then the "debit response" message indicates as such.

In step 620, card 5 sends a success message 320 along with the card signature back to client module 224 in client terminal 204. This success message may also be termed a "debit response" message. At this point, the purchase amount has been deducted from the balance on stored-value card 5. Next, in step 622. client module 224 packages the success message along with the card signature and sends them back to payment server 206 as indicated at 322. Client module 224 also logs the result of this stored-value card debit.

In step 624 the payment server receives incoming message 322 and creates a log and updates the transaction status in its database for future error recovery. The payment server then directs this received message to the security card in the terminal as indicated at 324. Next, in step 626 the security card processes this response from the client's terminal and verifies the received stored-value card signature.

As the security card contains the keys and algorithms necessary to compute stored-value card signatures, the security card is able to validate that a received stored-value card signature is in fact a valid one by comparing this stored-value card signature with a generated expected value. A successful comparison indicates that a success message 324 received from the stored-value card is in fact a valid success message and that the stored-value card has been debited. An error result

code or a comparison that is not successful potentially indicates that the stored-value card has not been debited by the proper amount. This comparison of stored-value card signatures by the security card ensures that a stored-value card is in fact debited before the merchant server is directed to release the purchased merchandise. This comparison of the stored-value card signature to an expected value is performed by the security card for the highest level of security. As will be described in the embodiments of FIG. 6, 7, and 8, this comparison of stored-value card signatures may also take place in the payment server, in the client terminal or in the merchant server with a variety of other advantages. Assuming that the transaction is so far valid, in step 628 the security card sends a "confirmation" message back to the payment server as indicated at 326. This confirmation message may also be termed a "message result."

In step 630 the terminal updates its data store with the stored-value card number, a transaction count, the total sale amount, the response from the security card, and transaction numbers from the stored-value card and from the security card. The payment server also logs the response received from the terminal including the merchant identifier, etc., as indicated in step 632. Next, in step 634, the payment server creates a confirmation message including the transaction identifiers and sends this message to the client terminal in encrypted form as indicated at 328. This message 328 may also be termed a "message result."

By sending this confirmation message in encrypted form, the confirmation message may be passed to the merchant server by way of the client terminal without fear of tampering. As the confirmation message is encrypted, it would be extremely difficult for the client terminal or another entity to forge a confirmation message and trick the merchant server into thinking that a transaction had taken place. In another embodiment of the invention, if the client terminal is a trusted agent, then the confirmation message need not be encrypted. In yet another embodiment, the payment server may sent two confirmation messages, one not encrypted for the client to process, and one encrypted for the merchant server. FIGS. 15A and 15B present an embodiment in which the payment server sends two messages to the client terminal.

At this point, the transaction thread of the payment server that was used for the current transaction may release the terminal, thus allowing the terminal to be used by other transactions. This transaction thread then exits at this time.

In step 636 the client terminal then passes this confirmation message

330 on to the merchant server at the URL address previously received from the merchant server. Message 330 may also be termed a "message result." The client may also post a message to the user informing that the debit has been completed. The client also logs confirmation of the payment. In step 638 the merchant server registers this confirmation message and checks for success. The merchant server calls a validate routine within the merchant code module with the confirmation message in order to validate the response from the client. The validate routine is able to take the transaction identifier along with the encrypted confirmation message to decrypt the confirmation message. If the decrypted confirmation message is acceptable, the merchant server then determines a successful transaction has occurred. Next, in step 640 the merchant server generates an HTML page with the purchased information and delivers this information to the client terminal. Alternatively, the merchant server may generate a purchase receipt to deliver to the client terminal indicating goods and/or services to be rendered. At this point, the client terminal may also log the merchant server's response. Completion of these steps indicates a successful financial transaction over the Internet using a stored-value card.

Returning now to a more detailed discussion of step 614, FIG. 11D describes one technique for processing a draw request message in conjunction with a security card. Once this draw request message has been received by the payment server and passed along to the terminal, the terminal parses the message back into individual responses and passes these responses sequentially to the security card as will be explained below. In an alternative embodiment, a dumb terminal is used and the draw request is parsed into its components and otherwise processed by the payment server, which then sends the responses to the security card itself.

In step 680 the payment code module of the payment server edits the draw request for syntactic correctness and logs the draw request message as being received. In step 682 the draw request is passed to the terminal interface module of the payment server. In one specific embodiment, the terminal interface then requests a terminal from the payment server's terminal pool. The payment server has a pool of terminals connected to the terminal concentrator that is established at start-up. At start-up, the payment server receives a list of all valid terminal identifiers. The payment server uses these identifiers, and its knowledge of transactions in progress to determine an appropriate terminal to process the transaction. Once a terminal is determined, the terminal interface builds a terminal specific message based upon the draw request and the type of terminal.

In step 686 the terminal specific draw request 312 is sent to the chosen terminal via the concentrator over a local area network. The concentrator acts as a router between a transaction thread in the payment server and its corresponding terminal. The concentrator looks at a header

on the draw request to determine to which terminal the transaction should be routed. In one embodiment of the invention, concentrator 212 is removed and payment server 206 communicates directly with terminal 214 (for example).

In step 688 the terminal parses the draw request message into its various components and processes each component in turn to emulate a stored-value card interacting with the security card in a physical terminal. Prepackaging of a variety of information into the draw request message results in fewer exchanges over the Internet between the client terminal and the payment server. By now simulating an interaction, the security card behaves as if it were in a physical terminal along with the stored-value card. A variety of responses from a stored-value card may be emulated. In this embodiment, the terminal sends each of the three packages "answer to reset", "initialize IEP". and "debit" down to the security card individually and waits for a return message before sending the next response. For a public key transaction, the certificates read by the client are also included as individual responses. In this fashion, even though all of the stored-value card information (the draw request) originating from the client terminal has been sent at once in prepackaged form over the Internet, the traditional interaction between the stored-value card and the security card in a physical terminal may be simulated at the terminal in a remote location.

In step 690 the terminal reaches a "draw amount" state, indicating that the security card is able to generate a debit command. In step 692, the security card generates its security card signature and the debit command. The debit command may also be termed a "debit IEP" command. This signature and debit command 314 are sent to the terminal. The debit command issued by the security card may contain a wide variety of information including the security card identifier, the transaction identifier, the amount to be debited, the currency and currency exponent for the amount, the security card signature, the date, time, and location. The terminal in turn, sends the signature, command, and the

terminal identifier to the payment server as indicated in step 694. The information may be sent to the payment server as indicated at 314 via a concentrator. At this point, step 614 ends and control returns to step 616.

FIRST ALTERNATIVE PAYMENT EMBODIMENT

FIG. 6 illustrates an alternative embodiment 200a in which the security card is able to be released sooner than the security card of FIG. 5; this embodiment also requires fewer exchanges between the terminal and the payment server. A security card in a terminal is dedicated to a particular transaction from the moment when the terminal interface selects that terminal until the security card finally issues a "confirmation" message and is released by a terminal interface. Thus, in some circumstances it is desirable to release the security card earlier. By releasing a security card earlier, the card is tied up for a shorter time per transaction and may move on to the next transaction sooner. Also, the less time that a terminal is dedicated to a particular transaction, and the fewer messages exchanged between the two, the less likely chance there is of a communication error that might interrupt and halt the transaction.

Embodiment 200a includes a client terminal 204, a payment server 206, a merchant server 208, a stored-value card 5, and a terminal 214 having a security card 218. Communication between the various entities may take place in a similar fashion as in FIG. 5 as indicated by communication links 234, 235, and 236. However, instead of two round trips of information between the terminal and payment server, there is only one round trip in this embodiment.

FIG. 12 is a flowchart that describes a technique for implementing this embodiment with reference to FIG. 6. Step 702 indicates that communication between the various entities takes place in a similar fashion as in FIG. 5 up until the terminal reaches the "draw amount" state. At this point, draw request 312 has been received and processed by the security card. Next, in step 704 the security card generates not only the security card signature and the debit command, but also an expected stored-value card signature. This expected stored-value card signature is a value expected by the security card from the stored-value card to validate the stored-value card's success message. This validation will ensure that the stored-valued card has in fact debited itself.

In step 706 the security card signature, the debit command and the expected stored-value card signature are sent to the payment code module in the payment server as indicated at 314a. Also, the terminal updates its data store in a similar fashion as in step 630. Next, step 708 indicates that the transaction occurs as before with reference to step 616-622. The steps indicate that the stored-value card receives the debit command, debits itself, and returns the success message (also termed a "debit response" message) and its card signature to the payment server. Next, in step 710 the payment server code module processes this response from the stored-value card by comparing 346 the received card signature with the expected stored-value card signature received earlier from the security card. This comparison of the two signatures by the payment module of the payment server foregoes the need for another round trip between the payment server and the security card. Because the security card has already delivered the expected card signature to the payment server, the security card may be released as soon as message 314a is received.

Assuming that the comparison is successful, the payment module is then able to generate its own confirmation message instead of waiting for a "confirmation" message from the security card. Next, step 712 indicates that the processing continues in a similar fashion as in steps 632-640. The confirmation message is passed on to the merchant server by way of

the client terminal and the merchant server may then deliver the purchased merchandise to the user.

SECOND ALTERNATIVE PAYMENT EMBODIMENT

In another embodiment 200b of the present invention as illustrated in FIG. 7, not only is the security card allowed to release earlier, but the number of messages exchanged between the client terminal and the payment server are reduced. Instead of comparing stored-value card signatures in the payment server, the expected stored-value card signature from the security card is transmitted to the client terminal where a trusted agent 356 performs the comparison of the expected stored-value card signature with the actual signature received from stored-value card 5. Thus, message exchange between the client terminal and the payment server is reduced to one round trip. This is advantageous in that the time for a

transaction is reduced, the security card is released earlier and fewer message exchanges means more reliability over the Internet.

Embodiment 200b includes a client terminal 204, a payment server 206, a merchant server 208, a stored-value card 5, and a terminal 214 having a security card 218. Communication between the various entities may take place in a similar fashion as in FIG. 5 as indicated by communication links 234 and 235.

FIG. 13 is a flowchart that describes a technique for implementing this embodiment with reference to FIG. 7. Step 722 indicates that communication between the various entities takes place in a similar fashion as in FIG. 5 up until the terminal reaches the "draw amount" state. At this point, draw request 312 has been received and processed by the security card. Next, in step 724 the security card generates not only the security card signature and the debit command, but also an expected stored-value card signature.

In step 726 the security card signature, the debit command and this expected stored-value card signature are sent to the payment code module in the payment server as indicated in 314a. Also, the terminal updates its data store in a similar fashion as in step 630. Next, in step 728 the payment server code module sends the debit command, merchant signature and expected stored-valued card signature to the client terminal.

Next, step 730 indicates that the transaction occurs as before with reference to steps 618 and 620. The steps indicate that the stored-value card receives the debit command and debits itself. In step 732, the client code module itself compares the actual card signature from the stored-value card with the expected signature from the security card. This comparison of the two signatures by the client module of the client terminal foregoes the need for another round trip between the payment server and the client terminal. Also. because the security card has already delivered the expected card signature to the payment server, the security card may be released as soon as message 314a is received. Assuming that the comparison is successful, the client terminal is then able to generate its own confirmation message in step 734 instead of waiting for a confirmation message from the payment server. Next, step 736 indicates that the processing continues in a similar fashion as in steps 636-640. The confirmation message is passed on to the merchant server and the merchant server may then deliver the purchased merchandise to the user.

THIRD ALTERNATIVE PAYMENT EMBODIMENT

FIG. 8 illustrates another embodiment 200c of the invention in which the merchant server performs the comparison of the stored-value card signature with the expected signature. This embodiment has all of the advantages of the previous embodiment in which the security card is released earlier, and there are also fewer messages passed between the entities. In this embodiment, if the client terminal is not to be trusted

to compare the stored-value card signatures, then an encrypted signature is passed to the merchant server via the client terminal. The client terminal also passes the raw, unencrypted signature from the stored-value card to the merchant server. A routine 366 in the merchant server then compares the two signatures.

Embodiment 200c includes a client terminal 204, a payment server 206, a merchant server 208, a stored-value card 5, and a terminal 214 having a security card 218. Communication between the various entities may take place in a similar fashion as in FIG. 5 as indicated by messages 302-306 and communication link 235.

FIG. 14 is a flowchart that describes a technique for implementing this embodiment with reference to FIG. 8. Step 742 indicates that communication between the various entities takes place in a similar fashion as in FIG. 5 up until the terminal reaches the "draw amount" state. At this point, draw request 312 has been received and processed by the security card. Next, in step 744 the security card generates not only the security card signature and the debit command, but also an expected stored-value card signature.

In step 746 the security card signature, the debit command and this expected stored-value card signature are sent to the payment code module in the payment server as indicated in 314a. Also, the terminal updates its data store in a similar fashion as in step 630. Next, in step 748 the payment server code module sends the debit command, merchant signature and an encrypted expected stored-valued card signature to the client terminal. The expected stored-valued card signature is encrypted to prevent tampering by the client terminal or other outside entity.

Next, step 750 indicates that the transaction occurs as before with reference to steps 618 and 620. The steps indicate that the stored-value card receives the debit command and debits itself. In step 752, the client code module sends the success message, the raw stored-value card signature and the encrypted signature on to the merchant server. In step 754 the merchant server processes the success message, decrypts the encrypted signature, and compares the two signatures. This comparison of the two signatures by the merchant server foregoes the need for another round trip between the payment server and the client terminal. Also, because the security card has already delivered the expected card signature to the payment server, the security card may be released as soon as message 314a is received.

Assuming that the comparison is successful, the merchant server is then able to generate its own confirmation message in step 756 instead of waiting for a confirmation message from the client terminal. Next, step 758 indicates that the processing continues in a similar fashion as in steps 638 and 640. The merchant server may then deliver the purchased merchandise to the user. In all of the above alternative embodiments, when the transaction is not completed successfully, the payment server reverses the transaction within the terminal.

ENCRYPTION LAYER EMBODIMENT

FIG. 9 illustrates an embodiment 200d of the present invention in which an encryption layer has been added. Although the present invention may be practiced without this added encryption layer, in a preferred embodiment of the invention, this encryption layer is used. FIG. 9 includes client terminal 204, payment server 206 and merchant server 208. Other elements of the architecture have been omitted in this figure for simplicity. This extra encryption layer is used not only to protect the contents of messages being transmitted over the Internet, but also to prevent a client terminal, stored-value card or other entity from receiving or producing a message that would trick another entity into thinking that a valid transaction had occurred. This encryption also prevents messages from being accidentally or deliberately altered or misdirected.

It should be appreciated that encryption may be present in any embodiment on all parts of any message sent for security. Preferably, any signature sent over a network is encrypted.

Figures 15A and 15B are a flowchart describing this embodiment of the invention with reference to FIG. 9. In step 802, the payment server and the merchant server share a unique encryption key. Through a prior business arrangement, both of the servers have arranged to share this unique key to add security to the transaction. The shared key may be of any suitable encryption standard and of any length. The key may be a Data Encryption Standard (DES) key having a length of 128 bits including parity. Although this shared key could be used directly, in a preferred embodiment of the invention, there is a derived unique key for each transaction between the merchant server and the payment server. Alternatively, another encryption standard such as RSA may also be used. Preferably, loading of value is performed under DES, while a purchase may be performed under either DES or public key technology.

In step 804 the client terminal and the merchant server engage in a protected Secure Sockets Layer (SSL) session 404 in which a connection is made, a user browses and makes a purchase selection. The SSL session protects the information transmitted over the Internet such as card information, commands, and encryption keys from being discovered by an unauthorized party. Other techniques for protecting a session may also be used.

In step 806 the merchant server derives a key from the DES key using information unique to the transaction such as the merchant identifier, the transaction identifier, or other information unique to this transaction, such as a random number. Because the payment server shares the DES key with the merchant server and also has access to this unique information about the transaction, the payment server will also be able to derive this same key from the shared DES key. In this step the merchant server also creates a transaction session key (TSK) for use by the client terminal and payment server in encrypting information.

In step 808 the merchant server downloads an HTML page of information 406 that includes the TSK and the TSK that is encrypted using the derived key (ETSK). The TSK encrypted with the derived key will be used by the payment server to return an encrypted (and unreadable by the client) confirmation message to the merchant server. Only the merchant server will be able to decrypt this confirmation message and will thus be guaranteed that a successful transaction has occurred and that merchandise may be released to the client.

In step 810, the client prepares the draw request in conjunction with the stored-value card and sends the draw request 408 encrypted with the TSK to the payment server along with the ETSK. In step 812 the payment server uses the shared DES key and the prearranged information unique to

the transaction to derive the same key that the merchant server has used. Thus, the derived key can be used to decrypt the ETSK in order to produce the TSK. Once the payment server had produced the TSK, it may decrypt the draw request and process the draw request in any suitable fashion with the security card. Once the payment server has received the debit command from the security card, it encrypts the debit command with the TSK. The debit command may also be termed the "debit IEP command."

In step 814 the payment server sends the encrypted debit command 410 to the client terminal. In step 816 the client decrypts the debit command with the TSK it had received earlier from the merchant server and processes the debit command in a suitable fashion with a stored-value card. Once the client terminal has received the debit response message from the stored-value card, it encrypts this message with the TSK and sends the debit response message 412 to the payment server. In step 820, the payment server decrypts the debit response message with the TSK and

processes the debit response message in a suitable fashion with the security card.
Once the payment server has received a "debit result" message from the security card, the payment server encrypts the "debit result" message with the TSK to form a "debit result C" message for the client. The "debit result C" message will be used by the client terminal to inform the user of a successful transaction. The payment server also generates its own confirmation message and encrypts the confirmation message with the derived key to form a "debit result M" message. The payment server then sends 414 the "debit result C" message and the "debit result M" message to the client terminal.
In step 822 the client terminal decrypts and processes the "debit result C" message and passes the "debit result M" message 416 on to the merchant server. Because the "debit result M" message is encrypted with the derived key, the client terminal or other entity is not able to tamper with it. In step 824 the merchant server is able to decrypt the ''debit result M" message because it had originally produced the derived key from the DES key. Once the merchant server has determined that a valid "debit result M" message has been received, it confirms that a valid transaction has taken place and may release merchandise to the user.
This security embodiment of FIG. 9 may be used with any of the previously described embodiments of the invention. By way of example, this security embodiment may be used with the embodiments of Figures 7 and 8 in which there is only one round trip between the client terminal and the payment server. In particular, the expected stored-value card signature received from the security card may be encrypted with the derived key so that it unreadable by the client, yet the merchant server will be able to compare the received stored-value card signature with the expected card signature to validate the transaction.
A wide variety of terminology may be used to describe the keys described above. For example, the keys referred to above as shared DES key, transaction session key (TSK) and derived key, may also be referred to as shared key, session C key and session M key.

AUTHENTICATION EMBODIMENT
FIG. 16 illustrates an architecture and system 200' for authentication over an internet (such as the Internet) using a pseudo stored-value application. This application could reside on a stored-value card along with standard accounts, stored value, or other card applications. The card defines access to the pseudo stored-value service and ensures that the card is present and passes security checks.
In one embodiment of the present invention, a consumer may wish to access any of a variety of Web servers in order to redeem **frequent flyer miles** , award points, etc., that he or she has **accumulated** . In this embodiment, a consumer has accumulated "points" through any of a variety of programs with airlines, restaurants, rental car companies, hotels, banks, **credit** or debit card issuers, telephone or other communication **company** , etc. The consumer wishes to redeem these points to receive free airline tickets, meals, car rental, overnight stays, prizes, awards, discounts, or other "benefits". By accessing a Web server associated with the particular program, the consumer is able to use his or her card in any of the embodiments described herein to authenticate the card and to receive these benefits from the program. Most often, a card has a card number that is associated with the consumer's name in a database on the Web server. This card number is transmitted to the Web server as part of the card signature, or in a similar fashion. Thus, an authenticated card used in this embodiment to redeem services may be matched to the appropriate consumer.
For example, a consumer with 30,000 frequent flyer miles on one airline

may use this embodiment of the present invention to access a Web server associated with the airline. The consumer is requesting a free round-trip ticket in exchange for 20,000 miles. The present invention then operates to authenticate the consumer's stored-value loyalty application on the card, and delivers a confirmation of authentication message to the Web server for the airline. The Web server then deducts 20,000 miles from the consumer's account (leaving 10,000 miles) and delivers the free ticket to the consumer. In one specific embodiment, the Web server associated with the airline (or the airline itself) keeps track of the consumer's account and deducts the mileage. In this instance, an authentication application is used to validate the presence of the card or to obtain access to the Web server site.

In another specific embodiment, the consumer's card contains a loyalty application that stores the consumer's accumulated frequent flyer mileage; the mileage from the card is then debited and confirmed to the Web server in a similar fashion as described in various of the embodiments by which a cash value is stored on and debited from a card.

System 200' may be implemented in a similar fashion as system 200 of FIG. 4. The elements shown in system 200' having counterparts in system 200 are described above and have similar functionality. System 200' includes a web server 208' that may be any suitable computer server capable of presenting award information (hereinafter "benefits") to a consumer over an open network such as the Internet. Web server 208' may be the same as merchant server 208 of FIG. 4 or a separate computer. Preferably, web server 208' is implemented in a similar fashion as described above for merchant server 208. Web server 208' includes server module 232' that is preferably implemented in a similar fashion as merchant module 232. Additionally, server module 232' includes functionality to store and present benefits that are available for particular consumers. For example, benefits available such as airline tickets, prizes, etc., may be presented.

Points (such as frequent flyer miles, for example) that a consumer accumulates to achieve benefits may be linked to a particular consumer by an account number, password, or other identifier. The amount of points accumulated for each consumer may be stored on web server 208' using server module 232', or may be located in another database of the organization providing the benefits. In an alternative embodiment, these points for each program that a consumer is enrolled in are stored in a loyalty application on the consumer's card. For example, a consumer may have a stored-value card that in addition to storing monetary value, also stores a quantity of frequent flyer miles accumulated for a particular airline (or a number of airlines), points accumulated for using a particular credit card, points for hotel stays at particular hotels, etc. For points stored on the consumer's loyalty application card, these points may be verified and debited in much the same way that monetary value on the consumer's card is debited as described herein.

One embodiment by which a consumer has his or her pseudo stored-value application on a card authenticated to redeem points for benefits will now be explained. In one specific embodiment, a technique similar to that described in the flowchart of FIGS. 11 A-11D for debiting monetary value may be used. Initially, a user (consumer) operating client terminal 204 accesses web server 208' over link 234', views benefits presented for a particular program (such as an airline's frequent flyer program), selects benefits from that program, and requests the transaction to be performed using his or her pseudo stored-value application to validate that the card has access to the services. Web server 208' receives and processes this request. The above steps may be performed in a similar fashion as steps 602 and 604.

Next, similar to step 606, web server 208' sends a page of information to client terminal 204. When claiming benefits, the total cost field is

zero and the currency field is a specially assigned value. Keeping total cost field equal to zero causes the system to perform authentication but not to create a payment record. Alternatively, for those user's whose card holds the amount of their points, additional fields may be sent from server 208' to terminal 204 indicating which account to debit and by how many points. The total cost and currency fields may be readily adapted for this purpose.
Next, in a similar fashion to steps 608 - 612, a draw request message is built, and the draw request is sent to authentication server 206' over link 236'. Similar to step 614, the authentication server now processes the draw request in conjunction with security card 218 (for example) and sends back a "debit" command and a security card signature to authentication server 206'. As total cost is zero, the "draw amount" state reached by security card 218 is also zero. In the alternative embodiment in which stored-value card 5 stores points for a particular

program, total cost may be a value and a "draw amount" state may be reached indicating a number of points to be deducted from card 5.
Next, similar to steps 616-618, authentication server 206' sends the debit command and security card signature to client terminal 204 and this information is processed by card 5. Even though a monetary value is not being debited, card 5 performs processing such as incrementing a counter indicating number of transactions and generating a stored-value card signature. In the alternative embodiment in which points are stored on card 5, the points needed to redeem the benefit chosen by the user from web server 208' may be debited from the appropriate account in this step.

Steps 620 through 638 are performed in a similar manner as in FIGS. 11B and 11C, except that in this case a monetary transaction is not being verified, but rather card 5 is being authenticated to allow the user to complete his access to services or benefits. In step 626 in particular, the signature of card 5 is verified by security card 218. In this embodiment, security card 218 would send an "authentication OK" message rather than the "confirmation" message of step 628. Web server 208' then debits the appropriate number of points from the user's account or allows access to a privileged service for the benefit requested. In the alternative embodiment in which points are stored on card 5, the "authentication OK" message serves not only as an authentication of card 5, but also confirmation that the correct number of points have been debited from card 5 for the appropriate program. Next, similar to step 640, web server 208' releases the benefit requested by the user (such as airline tickets, prizes, discounts, etc.) and the benefit is arranged to be delivered to the user.
It should be appreciated that this technique of redeeming points for benefits may also be practiced using any of the alternative embodiments of FIGS. 6, 7 or 8, thereby obtaining the advantages associated with those embodiments. Furthermore, this technique may take advantage of the encryption layer embodiment of FIG. 9. Additionally, as described below, the present invention may also be used to load more points onto card 5 in much the same way that monetary value is added.

LOADING A STORED-VALUE CARD
FIG. 17 illustrates a system 850 for loading value onto a stored-value card according to one embodiment of the present invention. System 850 includes a client terminal 204, bank server 860 and load server 862. Client terminal 204 communicates with card 5 via card reader 210, and with bank server 860 and load server 862 over any suitable open network such as Internet 202. Suitable embodiments for the client terminal, the card reader and the stored-value card are described above in the description of a payment technique. Preferably, each of client terminal

204, bank server 860 and load server 862 implement a code module (similar in operation to the code modules described above) in the Java programming language that provides the functionality described below. For simplicity of explanation, reference will be made below to "client terminal", "bank server" and "load server" even though the resident code is performing the functions. Card issuer 108 has been described previously in FIG. 3. Card issuer 108 may be a separate financial institution from the bank that includes bank server 860, or card issuer 108 may be the same bank that includes bank server 860.

Bank server 860 is any suitable computer within a bank or other financial institution. By way of example, bank server 860 is any suitable personal computer, a workstation or a mainframe computer. In one embodiment, bank server 860 runs a "servlet" program (a Java applet running on server) for communication with client 204.

Load server 862 is also any suitable computer and may be located at a third party location (such as at a processor) or may be located within the same bank as bank server 860. Load server 862 also runs a servlet program for communication with client terminal 204 and host security module 864. In an alternative embodiment, load server 862 and bank server 860 are the same computer which runs two different applications representing the functionality of each server.

Host security module (HSM) 864 is a device known in the art that may be embodied in a hardware "black box" or on any suitable computer. The host security module can be implemented in a hardware module outside of load server 862, can be implemented within load server 862, can be implemented in software, or can be implemented as a security card described above. Host security module 864 contains the encryption keys in hardware used for generating signatures (for example S1, S2 and S3) that provide security for the transaction. These signatures are used by stored-value card 5 and host security module 864 to insure that the card is not expired or counterfeit (i.e., is a valid card), to insure that module 864 is authentic, to insure that system 850 is authentic and, in general, to provide for a valid transaction and to prevent fraud. Card 5 also includes encryption keys for the generation of a stored-value card signature. In an alternative embodiment, module 864 could be replaced by a standard terminal that includes a security card such as is shown in the previous embodiments. In this situation, the encryption keys would be stored in the security card.

Briefly, system 850 operates as follows. A consumer accesses bank server 860 via client terminal 204. Assuming that card 5 is not overloaded and that the user's account with the bank has sufficient funds, the user is able to download value via bank server 860 on to his stored-value card 5. Client terminal 204 communicates with load server 862 to receive authorization for the load and for higher security. Card 5 may then be used to make purchases over the Internet as described earlier in the application or may be used for purchases elsewhere. Once the bank has downloaded value to card 5, a corresponding amount of funds is transferred from the bank to card issuer 108.

Card issuer 108 places these funds in a holding pool. Once stored-value card 5 is used to make a purchase from a merchant, the transaction is captured and settled through a settlement service, such as VisaNet. The issuer bank decrements the funds pool for the amount of the purchase, which is paid to the merchant bank. The merchant bank pays the merchant for the transaction. Settlement may occur in any suitable fashion such as is known in the art and, in particular, may be implemented as previously described in FIG. 3.

LOADING DETAILED TRANSACTION FLOW

One embodiment of a technique by which a stored-value card is loaded over the Internet will now be described using the flowchart of FIGS. 18A

through 18D with reference to FIG. 17. Various of the steps below may occur in a different order; the following description is for illustration purposes. Interaction between client terminal 204 and bank server 860, and between client terminal 204 and load server 862, is preferably implemented in a similar fashion as between client terminal 204 and merchant server 208, and between client terminal 204 and payment server 206 as described above, respectively. Certain implementation details mentioned above with respect to payment are equally applicable to loading a stored-value card. Furthermore, the exemplary flow shown in the figures illustrates a successful transaction (although a negative result is also explained below in the text). For this reason, a "confirmation" message is referred to, which can more broadly be referred to as a "result" message (to reflect both the possibilities of success and failure of a load). Also, a "load success" message is referred to, which can also be referred to as a "confirmation" message, to reflect its status as either confirming a positive load result or a negative load result.

Initially, a suitable web browser of client terminal 204 is used by the user to access a bank server Internet site. In step 871 the user selects an option to load value onto card 5. In step 872 the bank server sends a request for card information (including current card balance and maximum card balance); client terminal 204 reads the current card balance, currency, and other card information via card reader 2 10 and returns the balance to bank server 860. In step 873 the bank server determines the maximum load value and verifies that enough funds are in the user's account to accommodate a load request.

In step 874 the bank server builds an HTML page that includes the following client applet parameters: the load value; the type of currency being used; the port and IP address of the load server; a unique transaction identifier used by both the load server and the bank server to track a transaction; a unique bank identifier assigned to the bank and known to the load server; and a session key. Other information may also be included such as the currency's exponent, a status URL address of the bank server used for communication from the client terminal, and other security information to ensure the identity of the bank server and the integrity of the message. Other process related information such as software release level, encryption methodology and keys may also be conveyed. Once this page has been built, the page is sent to the requesting client browser and triggers the activation of the client code module (in this example a Java applet) in the client terminal.

To determine the load value, the bank server requests that the user enter the amount to load to the card. Assuming that the user's account is adequate, the bank server requests the user's account be debited in step 875 by the load value. Advantageously, the debit request from the bank server can use the existing ATM and accounting systems of the bank to debit the user's account. From the bank's point of view, value is being transferred from the user's account much in the same way that value would be transferred to a user in the form of cash at an ATM. In this situation, though, the value is not being dispensed as cash at an ATM,

but is being sent over the Internet to a stored-value card.

In step 876 the client terminal interacts with stored-value card 5 to obtain card information in order to build a load request message for later transmission to load server 862. Once responses from the card are received, the client terminal combines these responses into a byte stream suitable for transmission over a network to a load server.

The client terminal emulates a variety of host security module 864 commands to receive responses from these commands from the stored-value card. The stored-value card and the security module are physically separated from one another; communication takes place over the Internet. In the interest of speed and reliability, it is advantageous to have only

the traditional authentication, response, and confirmation messages exchanged.
To operate securely and reliably in this environment, in one embodiment of the present invention the client terminal emulates a security module and gathers all the responses for transmission into one load request message. The load request message may include a variety of information and preferably includes a first card signature (termed S 1), a card number, an expiry date and a load amount. Other information such as the security algorithm, transaction counter, current card balance, and bank server time stamp are also preferably provided.
As all of this information is prepackaged into a single load request message, the number of messages exchanged between the stored-value card and the security module over the Internet is minimized.
Next, in step 877 the client terminal accesses the load server using the IP address received from the bank server. In step 878 the client terminal sends the load request message to the load server. In step 879 the load server processes the load request in conjunction with an associated host security module 864 as will be explained in greater detail below with reference to FIG. 18D. After step 879, the load server has received an issuer security module signature (termed S2) as part of a load command from the security module 864. The security module signature is a value that uniquely identifies and validates the security module to prove to stored-value card 5 that the incoming load command is a valid command from a real security module. Thus, the user of the stored-value card, and other interested parties are guaranteed that a valid load of the card has occurred. In a preferred embodiment of the invention, the security module signature is an encrypted value ensuring that no other entity can forge an identity of a security module.
In step 880 the load server sends the load command including with the security module signature to the client terminal for the stored-value card to load itself. In step 881, upon receiving the load command from the load server, the client terminal passes the load command to stored-value card 5 which verifies the signature, loads itself by the load value, and also generates a load success message, a second stored-value card signature (termed S3), and a result code indicating success or failure of the load. In a preferred embodiment of the invention, this signature is in encrypted form to prevent tampering.
In step 882, card 5 sends load success message containing the card signature (S3) and result code back to client terminal 204. Next, in step 883 client terminal 204 packages the load success message along with the card signature and sends them back to load server 862. In step 884 the load server receives the incoming message. The load server then processes the message into its components and directs the components to the security module. Next, in step 885 the security module may process this response from the client's terminal and verify the received stored-value card signature (S3).
As the security module contains the keys and algorithms necessary to compute stored-value card signatures, the security module is able to validate that a received stored-value card signature is in fact a valid one by comparing the received stored-value card signature with a generated expected value. A successful comparison indicates that a load success message received from the stored-value card is in fact a valid success message and that the stored-value card has been loaded. Assuming that the transaction is so far valid, in step 886 the security module sends a "confirmation" message back to the load server.
It is possible that the stored-value card has not been loaded by the proper amount, that the card is invalid, a user is fraudulent or another discrepancy. For example, it is possible that a user has tampered with the card to make it appear that a load has not occurred, when in fact a load has occurred. In this situation, processing in step 882 and on is

slightly different. For example, instead of generating a "load success" message, the card my generate a "negative result" code, potentially indicating that the card has not been loaded. Processing of this situation would then occur as follows.

In step 882, card 5 sends a load message containing the result code and stored-value card signature S3 back to client terminal 204. Client terminal 204 recognizes a negative result code, and invokes negative result handling. Client terminal 204 interacts with card 5 and generates a new load request for a zero value load using elements from the original request, along with a new card signature S1.

The negative result code, along with the signatures S3 and new S1, and the zero value load request are passed to the load server for analysis. The load server determines if the transaction counter in the zero value load equals the transaction counter in the previous request, along with verifying other pertinent information such as date and time, card number, and currency code and exponent. If the transaction counters are the same, then it is possible that a valid negative result has been received, but it should be verified because the client is not trusted. If the counters are equal, the load server will hold the original S3 and will generate a new load request to the security module using data element values that would have been expected if the original transaction had failed. The new load request along with the new S1 is sent to the security module. The security module then compares the original S1 (from the original load request) to the new S1. If S1 is valid, then the original negative result is true and the security module generates a signature to confirm to the load server that there was no load. The original negative result from the card is then released to the security module to complete the original transaction. Processing would continue, but a user account would not be debited, and no settlement need occur because the card was, in fact, not loaded. If S I is not valid, the negative response is not true and then the result code in the original request is changed to reflect a successful load and passed to the security module. Processing then continues reflecting that a load has occurred.

On the other hand, if the transaction counters are not the same, then it is still possible that a valid negative result has been received, but it should be verified because the client is not trusted. First, the load server decreases the transaction counter in the new load request to match that of the original. The request along with the new S1 is passed to the security module. The security module calculates its own new S1 based upon the modified new load request. If there is no match, it means that the negative result was in error and that the card had been loaded. Processing continues to reflect a loaded card. If there is a match, it means the negative result was correct and that the transaction counter had been increased by accident. The user account is not debited, and not settlement occurs.

Returning now to further processing, in step 887 the load server logs the response received from the security module and updates its database with the transaction identifier, the bank identifier, the load value, etc. In general, any of the plethora of information passing through the load server may be added to its database. Next, in step 890 the load server creates a confirmation message including the transaction identifier and sends this message to the client terminal in encrypted form. By sending this confirmation message in encrypted form, the confirmation message may be forwarded to the bank server by way of the client terminal without fear of tampering. As the confirmation message is encrypted, it would be difficult for the client terminal or another entity to forge a confirmation message and trick the bank server into thinking that a valid load had taken place.

In step 891 the client terminal forwards the confirmation message on to the bank server at the URL address previously received from the bank

server. The client terminal may also post a message to the user informing that the load has been completed. The client terminal also logs confirmation of the load. In step 892 the bank server registers the confirmation message. The bank server calls a routine to decrypt the confirmation message. If the decrypted confirmation message is acceptable, the bank server determines a successful load has occurred. The confirmation message provides assurance to the bank that the user's card was in fact loaded with a particular value and prevents fraud. For example, a fraudulent user who tries to claim that his bank account was decremented and his card not loaded (and should thus receive more money from the bank) would be thwarted because the confirmation message proves that the user's card was in fact loaded. Alternatively, the "confirmation" message may indicate that a load did not occur, in which case the account would not be debited, and no settlement would occur. At this point a successful load of the user's card has occurred (assuming all is well). For example, if the user had requested $100, that amount has been decremented from the user's account at the bank, and $100 has been loaded onto the user's stored-value card. Preferably, at this point the amount loaded (in this example $100) is transferred from the

bank to the stored-value card issuer preferably through an existing network. The $100 is transferred so that the card issuer may manage the float on these unspent funds until the user spends the $100. Once the $100 (or a smaller portion) has been spent with a merchant, the card issuer is then able to settle the transaction with the merchant using any suitable clearing and administration system. In alternative embodiment, the bank may retain the $100 and settle directly with the merchant. In another embodiment, the bank and the card issuer are the same financial institution, and the $100 may be shifted between parts of the organization or remain in place.

Returning now to a more detailed discussion of step 879, FIG. 11D describes a technique for processing a load request message in conjunction with a security module. Once the load request message is received by the load server, the load server parses it into the appropriate elements and passes a request to the security module as will be explained below. Alternatively, the load server can build a network message and switch the request to a remote authentication server. Or, a smart terminal could parse the message and pass responses to the security module.

In step 895 the load server edits the load request for syntactic correctness and logs the request as received. In step 896 the load server constructs a load request message. In step 897 the load server passes the load request to the security module to emulate a stored-value card interacting with the security module. The load server behaves as if a stored-value card were actually interacting in an ATM (for example) through a network to a host with a security module. In this fashion, the load request originating from the client terminal has been sent in prepackaged form over the Internet emulating a traditional interaction between the stored-value card in an ATM.

In step 898, the security module verifies the received stored-value card signature (S1) to prevent fraud. The security module generates its security module signature (termed S2) and the load command. The signature S2 will confirm to the client terminal and the stored-value card that the host security module is authentic and belongs to the issuer of the stored-value card. Additionally, S2 protects against a user trying to perform a fake load, keys out of synchronization, a counterfeit card, an expired card, etc. The security module then sends the signature and load command to the load server as indicated in step 899. At this point. step 879 ends and control returns to step 880.

In another embodiment of the loading technique, a consumer may wish to

access any of a variety of Web servers in order to load frequent flyer miles, award points, etc., that he or she has accumulated. A technique for authentication and redemption of such "points" is described above. In the loading embodiment, a consumer has accumulated points through any of a variety of programs with airlines, restaurants, rental car companies, hotels, banks, credit or debit card issuers, telephone or other communication companies, etc. These points are stored by the particular airline, etc., that has issued them. The consumer wishes to load these points onto his or her stored-value card in order to redeem them elsewhere; thus receiving airline tickets, meals, car rental, overnight stays, prizes, awards, discounts, or other benefits. By accessing an Internet server associated with the particular program, the consumer is able to load his or her stored-value card in any of the embodiments described herein to receive the benefits of the program, much in the same way that currency is loaded.

COMPUTER SYSTEM EMBODIMENT

FIG. 19 illustrates a computer system 900 suitable for implementing an embodiment of the present invention. Computer system 900 includes any number of processors 902 (also referred to as central processing units, or CPUs) that are coupled to storage devices including primary storage 906 (such as random access memory, or RAM) and primary storage 904 (such as a read only memory, or ROM). As is well known in the art, primary storage 904 acts to transfer data and instructions uni-directionally to the CPU and primary storage 906 is used typically to transfer data and instructions in a bi-directional manner. Both of these primary storage devices may include any suitable of the computer-readable media described below. A mass storage device 908 is also coupled bi-directionally to CPU 902 and provides additional data storage capacity and may also include any of the computer-readable media described below. Mass storage device 908 may be used to store programs, data and the like and is typically a secondary storage medium (such as a hard disk) that is slower than primary storage. It will be appreciated that the information retained within mass storage device 908, may, in appropriate cases, be incorporated in standard fashion as part of primary storage 906 as virtual memory. A specific mass storage device such as a CD-ROM 914 passes data uni-directionally to the CPU.

CPU 902 is also coupled to an interface 910 that includes one or more input/output devices such as such as video monitors, track balls, mice, keyboards, microphones, touch-sensitive displays, transducer card readers, magnetic or paper tape readers, tablets, styluses, voice or handwriting recognizers, biometrics readers, or other computers. CPU 902 optionally may be coupled to another computer or telecommunications network using a network connection as shown generally at 912. With such a network connection, it is contemplated that the CPU might receive information from the network, or might output information to the network in the course of performing the above-described method steps. Furthermore, method embodiments of the present invention may execute solely upon CPU 902 or may execute over a network connection such as the Internet in conjunction with a remote CPU that shares a portion of the processing.

In addition, embodiments of the present invention further relate to computer storage products with a computer readable medium that have program code thereon for performing various computer-implemented operations. The media and program code may be those specially designed and constructed for the purposes of the present invention, or they may be of the kind well known and available to those having skill in the computer software arts. Examples of computer-readable media include, but are not limited to: magnetic media such as hard disks, floppy disks, and magnetic tape; optical media such as CD-ROM disks; magneto-optical media

such as floptical disks; and hardware devices that are specially configured to store and execute program code, such as application-specific integrated circuits (ASICs), programmable logic devices (PLDs) and ROM and RAM devices. Examples of program code include machine code, such as produced by a compiler, and files containing higher level code that are executed by a computer using an interpreter. Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. For instance, any suitable stored-value card capable of loading, storing and decrementing value on command may be used with the present invention. Also, any network capable of performing routing functionality between a client terminal and a load and bank server may be used. Furthermore, the security module may be a physically separate module, a card located in a terminal attached to a load server, or its functionality may be incorporated directly into a load server in hardware or software. And although the client terminal may be used to route messages between the bank server and load server, both of these servers may also communicate directly between themselves, and may even be the same computer. The specific messages shown passing between the computers are exemplary, and other types of messages may be used. A specified load request is shown, but other information may also be loaded onto a stored-value card using a security module emulation and then sent packaged as one message to the security module over a network. In addition to monetary value, other types of value such as electronic cash, checks, awards, loyalty points, benefits, etc., may be loaded onto a card, and the term "value" is intended to broadly cover all these various types. Any suitable type of encryption may be used to encrypt messages passing between the computers. Therefore, the described embodiments should be taken as illustrative and not restrictive, and the invention should not be limited to the details given herein but should be defined by the following claims.

CLAIMS EP 1023705 B1

1. A network payment system (200) for transacting a sale of merchandise over a network using a stored-value card (5), said network payment system comprising:

a router (202) for routing communication between entities attached to said network;

a merchant server (208) in communication with said network, said merchant server having at least a first item of merchandise for sale;

a client terminal (204) in communication with said network, said client terminal including a card reader (210) for communicating with said stored-value card, an output device (910) for reviewing said first item for sale, and an input device (910) for initiating a purchase transaction to purchase said first item for sale, said client terminal being arranged to build a purchase message (304) using information obtained from said stored-value card, said stored-value card being arranged to debit itself upon receiving a debit command (314) from a security card (220); and characterised by

a payment server (206) in communication with said network, said payment server including an interface for communicating with said security card and being arranged to receive said purchase message including an indication of said purchase transaction and to transmit a confirmation message (326) to said merchant server over said network

indicating that said stored-value card has been debited, said security card being arranged to create said debit command intended for said stored-value card, whereby said merchant server is

authorized to release said item of merchandise to a user associated with said stored-value card.
2. A network payment system as recited in claim 1 wherein said network is an internet (202) and said merchant server includes a merchant web site for advertising said first item for sale over said internet.
3. A network payment system as recited in claim 1 or 2 wherein said client terminal and said merchant server are at separate locations and communicate over said internet.
4. A network payment system as recited in claims 1-3 further comprising: a clearing and administration system (110) for reconciling a plurality of transactions over said network.
5. A network payment system as recited in any of claims 1-4 wherein said client terminal further includes a command emulator for emulating security card commands that are sent to said stored-value card and for grouping responses to said security card commands into a draw request message (310) to be sent to said payment server, and said payment server includes a response emulator for emulating responses from said stored-value card that are sent to said security card.
6. A network payment system as recited in any of claims 1-5 wherein said payment server includes a comparator for comparing a stored-valued card signature (324) received from said stored-value card with an expected signature (314) received from said security card to confirm a transaction, whereby the message traffic between said payment server and said security card is reduced.
7. A network payment system as recited in any of claims 1-5 wherein said client terminal includes a comparator for comparing a stored-valued card signature (320) received from said stored-value card with an expected signature (316) from said security card received via said payment server to confirm a transaction, whereby message traffic between said payment server and said client terminal, and between said payment server and said security card is reduced.
8. A network payment system as recited in any of claims 1-5 wherein said merchant server includes a comparator for comparing a stored-valued card signature (360) received from said stored-value card with an expected signature from said security card received via said payment server, whereby a transaction is confirmed and whereby message traffic from said payment server, and between said payment server and said security card is reduced.
9. A computer-implemented method of selling merchandise over a network (202) using a merchant server (208), said merchandise for purchase by a user with a stored-value card (5), said method comprising:
establishing communication (234) between said merchant server (208) and a client (204) over said network;
receiving a request from said client (204) to purchase an item available from said merchant server (208);
transmitting to said client a purchase amount of said item so that said client may build a draw request message (310) using information obtained from a stored-value card and debit said stored-value card associated with said client by said amount upon receiving a debit command (314) from a security card (220); characterised by
transmitting (236) said amount, a transaction identifier and a merchant identifier to a payment server (206) connected to said network, said payment server being associated with said security card that creates a debit command intended for said stored-value card and secures the purchase of said item, said transaction identifier uniquely identifying the purchase of said item and said merchant identifier uniquely identifying said merchant server to said payment server; and

a confirmation step (238) for performing the function of confirming said purchase of said item to said merchant server, whereby said merchant

server is informed that said sale of said item is a success and said merchant server may release said item to said user associated with said stored-value card.
10. A method as recited in claim 9, wherein said network is an internet (202) over which said recited steps of said method occur, wherein said merchant server includes a merchant web site for advertising said merchandise over said internet, and wherein said client terminal (204) and said merchant server (208) are at separate locations.
11. A method as recited in claims 9 or 10 further comprising:
transmitting a first key to said client for encrypting a draw request message to be sent to said payment server from said client terminal;
providing said first key to decrypt said encrypted draw request message to said payment server without sending said first key in the clear to said payment server; and
receiving an encrypted transaction confirmation message from said payment server that is encrypted by a second key shared between said merchant server and said payment server.
12. A method as recited in any one of claims 9 to 11, wherein said step of transmitting said purchase amount and said confirming step are routed through said client to provide communication between said merchant server and said payment server, whereby the number of communication links is reduced.
CLAIMS EP 1023705 B1
1. Netzwerkzahlungssystem (200) zum Abwickeln eines Warenverkaufs uber ein Netzwerk unter Verwendung einer Guthabenkarte (5), umfassend:
einen Router (202) zum Routen der Kommunikation zwischen an das Netzwerk angeschlossenen Einheiten;
einen mit dem Netzwerk kommunizierenden Handlerserver (208), der uber zumindest einen ersten Warenposten zum Verkauf verfugt;
ein mit dem Netzwerk kommunizierendes Kundenterminal (204), das ein Kartenlesegerat (210) zum Kommunizieren mit der Guthabenkarte, ein Ausgabegerat (910) zum Prufen des ersten Verkaufspostens und ein Eingabegerat (910) zum Einleiten einer Kauftransaktion zum Kauf des ersten Verkaufspostens umfasst, wobei das Kundenterminal so aufgebaut ist, dass es anhand von Informationen, die von der Guthabenkarte erhalten werden, eine Kaufmeldung (304) erstellt, wobei die Guthabenkarte so aufgebaut ist, dass sie bei Erhalt eines Abbuchungsbefehls (314) von einer Sicherheitskarte (220) eine automatische Abbuchung von ihrem Speicherwert vornimmt; und
gekennzeichnet durch
einen mit dem Netzwerk kommunizierenden Zahlungsserver (206), der eine Schnittstelle zum Kommunizieren mit der Sicherheitskarte umfasst und so aufgebaut ist, dass er die Kaufmeldung einschlieslich einer Anzeige der Kauftransaktion erhalt und uber das Netzwerk eine Bestatigungsmeldung (326) an den Handlerserver ubertragt, die anzeigt, dass eine Abbuchung von der Guthabenkarte vorgenommen wurde, wobei die Sicherheitskarte so aufgebaut ist, dass sie den fur die Guthabenkarte bestimmten Abbuchungsbefehl erstellt, wodurch der Handlerserver autorisiert wird, den Warenposten an einen der Guthabenkarte zugewiesenen Benutzer auszugeben.
2. Netzwerkzahlungssystem nach Anspruch 1, wobei es sich beim dem Netzwerk um ein Internet (202) handelt und der Handlerserver eine Handlerwebseite zum Bewerben des ersten Verkaufspostens uber das Internet umfasst.
3. Netzwerkzahlungssystem nach Anspruch 1 oder 2, wobei sich das Kundenterminal und der Handlerserver an unterschiedlichen Standorten befinden und uber das Internet Informationen austauschen.
4. Netzwerkzahlungssystem nach Anspruch 1 bis 3, weiterhin umfassend:
ein Abrechnungs- und Verwaltungssystem (110) zum Abgleichen einer Vielzahl von Transaktionen uber das Netzwerk.

5. Netzwerkzahlungssystem nach einem der Anspruche 1 bis 4, wobei das Kundenterminal weiterhin einen Befehlsemulator zum Emulieren von Sicherheitskartenbefehlen, die an die Guthabenkarte gesendet werden, und zum Gruppieren von Antworten auf die Sicherheitskartenbefehle in eine an den Zahlungsserver zu sendende Abbuchungsanforderungsmeldung (310) umfasst, und wobei der Zahlungsserver einen Antwortemulator zum Emulieren von Antworten der Guthabenkarte umfasst, die an die Sicherheitskarte gesendet werden.
6. Netzwerkzahlungssystem nach einem der Anspruche 1 bis 5, wobei der Zahlungsserver einen Komparator zum Vergleichen einer Guthabenkartenunterschrift (324), die von der Guthabenkarte erhalten wurde, mit einer erwarteten Unterschrift (314), die von der Sicherheitskarte erhalten wurde, zur Bestatigung einer Transaktion umfasst, wodurch der Meldungsverkehr zwischen dem Zahlungsserver und der Sicherheitskarte reduziert wird.
7. Netzwerkzahlungssystem nach einem der Anspruche 1 bis 5, wobei das Kundenterminal einen Komparator zum Vergleichen einer Guthabenkartenunterschrift (320), die von der Guthabenkarte erhalten wurde, mit einer erwarteten Unterschrift (316), die von der Sicherheitskarte uber den Zahlungsserver erhalten wurde, zur Bestatigung einer Transaktion umfasst, wodurch der Meldungsverkehr zwischen dem Zahlungsserver und dem Kundenterminal sowie zwischen dem Zahlungsserver und der Sicherheitskarte reduziert wird.
8. Netzwerkzahlungssystem nach einem der Anspruche 1 bis 5, wobei der Handlerserver einen Komparator zum Vergleichen einer Guthabenkartenunterschrift (360), die von der Guthabenkarte erhaltene wurde, mit einer erwarteten Unterschrift, die von der Sicherheitskarte uber den Zahlungsserver erhalten wurde, umfasst, wodurch eine Transaktion bestatigt wird und wodurch der Meldungsverkehr vom Zahlungsserver sowie zwischen dem Zahlungsserver und der Sicherheitskarte reduziert wird.
9. Computer-implementiertes Verfahren zum Verkaufen von Waren uber ein Netzwerk (202) unter Verwendung eines Handlerservers (208), wobei die Waren fur den Kauf durch einen Benutzer mit einer Guthabenkarte (5) vorgesehen sind, umfassend:
das Herstellen der Kommunikation (234) zwischen dem Handlerserver (208) und einem Kunden (204) uber das Netzwerk;
den Empfang einer Anforderung vom Kunden (204) zum Kauf eines vom Handlerserver (208) verfugbaren Postens;
das Ubertragen eines Kaufbetrags fur den Posten an den Kunden, so dass

der Kunde unter Verwendung von Informationen, die von einer Guthabenkarte erhalten werden, eine Abbuchungsanforderungsmeldung (310) erstellen und bei Erhalt eines Abbuchungsbefehls (314) von einer Sicherheitskarte (220) diesen Betrag von der dem Kunden zugewiesenen Guthabenkarte abbuchen kann; gekennzeichnet durch
das Ubertragen (236) des Betrags, einer Transaktionskennung und einer Handlerkennung an einen mit dem Netzwerk verbundenen Zahlungsserver (206), wobei der Zahlungsserver der Sicherheitskarte zugewiesen ist, die einen fur die Guthabenkarte bestimmten Abbuchungsbefehl erstellt und den Kauf des Postens sichert, wobei die Transaktionskennung den Kauf des Postens und die Handlerkennung den Handlerserver eindeutig beim Zahlungsserver identifiziert; und durch
einen Bestatigungsschritt (238) zum Durchfuhren des Bestatigungsvorgangs des Kaufs des Postens beim Handlerserver, wodurch der Handlerserver daruber informiert wird, dass der Verkauf des Postens erfolgreich war und der Handlerserver den Posten an den mit der Guthabenkarte verbundenen Benutzer ausgeben kann.
10. Verfahren nach Anspruch 9, wobei es sich bei dem Netzwerk um ein Internet (202) handelt, uber das die genannten Schritte des

Verfahrens ausgefuhrt werden, wobei der Handlerserver eine Handlerwebseite zum Bewerben der Ware uber das Internet umfasst, und wobei sich das Kundenterminal (204) und der Handlerserver (208) an unterschiedlichen Standorten befinden.

11. Verfahren nach Anspruch 9 oder 10, weiterhin umfassend:
das Ubertragen eines ersten Schlussels an den Kunden zum Verschlusseln einer vom Kundenterminal an den Zahlungsserver zu sendenden Abbuchungsanforderungsmeldung;
das Bereitstellen des ersten Schlussels zum Entschlusseln der an den Zahlungsserver gesendeten, verschlusselten Abbuchungsanforderungsmeldung, ohne dass der erste Schlussel in offener Form an den Zahlungsserver gesendet wird; und
das Empfangen einer verschlusselten Bestatigungsmeldung fur die Transaktion vom Zahlungsserver, die anhand eines zweiten Schlussels verschlusselt wird, der vom Handlerserver und vom Zahlungsserver gemeinsam verwendet wird.

12. Verfahren nach einem der Anspruche 9 bis 11, wobei der Schritt des Ubertragens des Kaufbetrags und der Schritt des Bestatigens uber den Kunden geroutet werden, um so eine Kommunikation zwischen dem Handlerserver und dem Zahlungsserver bereitzustellen, wodurch die Anzahl der Kommunikationsverbindungen reduziert wird.

CLAIMS EP 1023705 B1

1. Un systeme de paiement par reseau (200) pour effectuer une vente de marchandise sur un reseau en utilisant une carte a valeur stockee (5), ce systeme de paiement par reseau comprenant :
un routeur (202) pour router une communication entre des entites connectees au reseau;
un serveur de commercant (208) en communication avec le reseau, ce serveur de commercant ayant au moins un premier article de marchandise a vendre;
un terminal client (204) en communication avec le reseau, ce terminal client incluant un lecteur de cartes (210) pour communiquer avec la carte a valeur stockee, un dispositif de sortie (910) pour examiner le premier article a vendre, et un dispositif d'entree (910) pour declencher une transaction d'achat pour acheter le premier article a vendre, ce terminal client etant concu pour construire un message d'achat (304) en utilisant de l'information obtenue a partir de la carte a valeur stockee, cette carte a valeur stockee etant concue pour se debiter a la reception d'un ordre de debit (314) provenant d'une carte de securite (220); et caracterise par
un serveur de paiement (206) en communication avec le reseau, ce serveur de paiement incluant une interface pour communiquer avec la carte de securite et etant concu pour recevoir le message d'achat incluant une indication de la transaction d'achat, et pour emettre un message de confirmation (326) vers le serveur de commercant sur le reseau, indiquant que la carte a valeur stockee a ete debitee, la carte de securite etant concue pour creer l'ordre de debit destine a la carte a valeur stockee, grace a quoi le serveur de commercant est autorise a remettre ledit article de marchandise a un utilisateur associe a la carte a valeur stockee.

2. Un systeme de paiement par reseau selon la revendication 1, dans lequel le reseau est un internet (202) et le serveur de commercant comprend un site Web de commercant pour proposer le premier article a vendre sur cet internet.

3. Un systeme de paiement par reseau selon la revendication 1 ou 2, dans lequel le terminal client et le serveur de commercant sont a des emplacements separes et communiquent par ledit internet.

4. Un systeme de paiement par reseau selon les revendications 1-3, comprenant en outre :
un systeme de compensation et d'administration (110) pour rapprocher une

multiplicite de transactions sur le reseau.
5. Un systeme de paiement par reseau selon l'une quelconque des revendications 1-4, dans lequel le terminal client comprend en outre un emulateur d'ordres pour emuler des ordres de carte de securite qui sont envoyes a la carte a valeur stockee, et pour grouper des reponses a ces ordres de carte de securite en un message de demande de debit (310) destine a etre envoye au serveur de paiement, et le serveur de paiement comprend un emulateur de reponse pour emuler des reponses provenant de la carte a valeur stockee qui sont envoyees a la carte de securite.
6. Un systeme de paiement par reseau selon l'une quelconque des revendications 1-5, dans lequel le serveur de paiement comprend un comparateur pour comparer une signature de carte a valeur stockee (324) recue de la carte a valeur stockee avec une signature attendue (314) recue de la carte de securite pour confirmer une transaction, grace a quoi le trafic de messages entre le serveur de paiement et la carte de securite est reduit.
7. Un systeme de paiement par reseau selon l'une quelconque des revendications 1-5, dans lequel le terminal client comprend un comparateur pour comparer une signature de carte a valeur stockee (320) recue de la carte a valeur stockee, avec une signature attendue (316) provenant de la carte de securite, recue par l'intermediaire du serveur de paiement pour confirmer une transaction, grace a quoi le trafic de messages entre le serveur de paiement et le terminal client, et entre le serveur de paiement et la carte de securite, est reduit.
8. Un systeme de paiement par reseau selon l'une quelconque des revendications 1-5, dans lequel le serveur de commercant comprend un comparateur pour comparer une signature de carte a valeur stockee (360) recue de la carte a valeur stockee, avec une signature attendue provenant de la carte de securite, recue par l'intermediaire du serveur de paiement, grace a quoi une transaction est confirmee, et grace a quoi le trafic de messages provenant du serveur de paiement, et entre le serveur de paiement et la carte de securite, est reduit.
9. Un procede mis en oeuvre par ordinateur pour vendre une marchandise sur un reseau (202) en utilisant un serveur de commercant (208), cette marchandise etant destinee a etre achetee par un utilisateur avec une carte a valeur stockee (5), ce procede comprenant :
l'etablissement d'une communication (234) entre le serveur de commercant (208) et un client (204) sur le reseau;
la reception d'une requete provenant du client (204) pour acheter un article disponible au serveur de commercant (208);
l'emission vers le client d'un montant d'achat dudit article, de facon que le client puisse construire un message de requete de debit (310) en utilisant de l'information obtenue a partir d'une carte a valeur stockee, et debiter dudit montant la carte a valeur stockee associee a ce client, a la reception d'un ordre de debit (314) provenant d'une carte de securite (220); caracterise par
l'emission (236) dudit montant, d'un identificateur de transaction et d'un identificateur de commercant, vers un serveur de paiement (206) connecte au reseau, ce serveur de paiement etant associe a ladite carte de securite qui cree un ordre de debit destine a la carte a valeur stockee, et assure l'achat dudit article, cet identificateur de transaction identifiant de maniere specifique l'achat dudit article, et l'identificateur de commercant identifiant de maniere specifique le serveur de commercant aupres du serveur de paiement; et

une etape de confirmation (238) pour remplir la fonction de confirmation de l'achat de l'article au serveur de commercant, grace a quoi le serveur de commercant est informe du fait que la vente dudit article

a reussi et que le serveur de commercant peut remettre ledit article a l'utilisateur associe a la carte a valeur stockee.
10. Un procede selon la revendication 9, dans lequel le reseau est un internet (202) sur lequel les etapes precitees du procede ont lieu, le serveur de commercant incluant un site Web de commercant pour proposer ladite marchandise sur l'internet, et dans lequel le terminal client (204) et le serveur de commercant (208) sont a des emplacements separes.
11. Un procede selon les revendications 9 ou 10, comprenant en outre : l'emission d'une premiere cle vers le client pour chiffrer un message de demande de debit destine a etre envoye au serveur de paiement a partir du terminal client;
la fourniture de la premiere cle pour dechiffrer le message de requete de debit chiffre adresse au serveur de paiement, sans envoyer la premiere cle en clair au serveur de paiement; et
la reception d'un message de confirmation de transaction chiffre, provenant du serveur de paiement, qui est chiffre par une seconde cle partagee entre le serveur de commercant et le serveur de paiement.
12. Un procede selon l'une quelconque des revendications 9 a 11, dans lequel l'etape d'emission du montant d'achat et l'etape de confirmation transitent a travers le client pour permettre une communication entre le serveur de commercant et le serveur de paiement, grace a quoi le nombre de liaisons de communication est reduit.

...SPECIFICATION may wish to access any of a variety of Web servers in

order to redeem **frequent flyer miles** , award points, etc., that he or she has **accumulated** . In this embodiment, a consumer has accumulated "points" through any of a variety of programs with airlines, restaurants, rental car companies, hotels, banks, **credit** or debit card issuers, telephone or other communication **company** , etc. The consumer wishes to redeem these points to receive free airline tickets, meals, car...

5/9,K/11 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00459194 **Image available**
INTERNET PAYMENT AND LOADING SYSTEM USING SMART CARD
SYSTEME DE PAIEMENT ET DE CHARGEMENT PAR INTERNET A L'AIDE D'UNE CARTE A PUCE
Patent Applicant/Assignee:
VISA INTERNATIONAL SERVICE ASSOCIATION,
DAVIS Virgil M,
CUTINO Suzanne C,
BERG Michael J,
CONKLIN Fredrick Sidney,
PRINGLE Steven John,
Inventor(s):
DAVIS Virgil M,
CUTINO Suzanne C,
BERG Michael J,
CONKLIN Fredrick Sidney,
PRINGLE Steven John,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9849658 A1 **19981105**
Application: WO 98US8806 19980430 (PCT/WO US9808806)
Priority Application: US 9745883 19970430; US 97951614 19971016

Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM GW HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Main International Patent Class (v7): G07F-019/00
International Patent Class (v7): G07F-07:10
Publication Language: English
Fulltext Word Count: 25424

English Abstract
An architecture and system loads and uses a smart card (5) for payment of goods and/or services purchased on-line over the Internet (202). A client module on a client terminal (204) controls the interaction with a consumer and interfaces to a card reader (210) which accepts the consumer's smart card (5) and allows loading and debiting of the card. Debiting works in conjunction with a merchant server (208) and a payment server (206). Loading works in conjunction with a bank server (860) and a load server (862). The Internet provides the routing functionality between the client terminal and the various servers. A payment server (206) on the Internet includes a computer and a security module (or a security card (218) in a terminal (214)) to handle the transaction, data store and collection. A merchant server (208) advertises the goods and/or services offered by a merchant for sale on a web site. The merchant contracts with an acquirer to accept smart card payments for goods and/or services purchased over the Internet. A consumer uses his smart card (5) at the client terminal (204) in oder to purchase goods and/or services from the remote merchant server (208). The client terminal sends a draw request to the payment server. The payment server processes, confirms and replies to the merchant server (optionally by way of the client terminal). To load value, the client terminal (204) requests a load from a user account at the bank server (860). A load request is sent from the card (5) to the load server (862) which processes, confirms and replies to the bank server (optionally by way of the client terminal). The bank transfers loaded funds to the card issuer (108) for later settlement for a merchant from whom the user purchases goods with value on the card.

French Abstract
L'invention porte sur une architecture et un systeme chargeant et utilisant une carte a puce (5) pour le paiement de marchandises et/ou de services achetes en ligne via Internet (202). Un module client du terminal client (204) gere les interactions avec un consommateur et sert d'interface avec un lecteur (210) de cartes qui accepte la carte a puce (5) du consommateur et permet de la charger et de la debiter. Le debit se fait en association avec un serveur commercial (208) et un serveur de paiement (206). Le chargement se fait en association avec un serveur bancaire (860) et un serveur de chargement (862). Le reseau Internet assure les fonctions d'acheminement entre le terminal client et les differents serveurs. Un serveur de paiement (206) du reseau Internet comporte un ordinateur et un module de securite (ou une carte de securite (218) situee dans un terminal (214)) pour traiter la transaction, stocker les donnees et les recueillir. Un serveur commercial (208) presente les marchandises et/ou services offerts par un commercant a la vente sur un site Internet. Le commercant se met d'accord avec un acquereur pour accepter les cartes a puce en paiement des marchandises et/ou services achetes via Internet. Un consommateur utilise sa carte a puce (5) au

terminal client (204) en vue de l'achat de marchandises et/ou de services au serveur commercial a distance (208). Le terminal client envoie une demande de retrait au serveur de paiement. Le serveur de paiement apres traitement confirme et repond au serveur commercial (facultativement via le terminal client). Pour charger des valeurs, le terminal client (204) fait au serveur bancaire (860) une demande de chargement depuis un compte utilisateur. Une demande de chargement est adressee par la carte (5) au serveur de chargement (862) qui apres traitement confirme et repond au serveur bancaire (facultativement via le terminal client). La banque transfert les fonds charges a l'emetteur de carte (108) en vue du reglement ulterieur du commercant auquel l'utilisateur a achete des marchandises avec des valeurs chargees sur la carte.

Detailed Description
INTERNET PAYMENT AND LOADING SYSTEM USING SMART CARD
FIELD OF THE INVENTION
The present invention relates generally to a payment system and a value loading system using a computer network. More specifically, the present invention relates to a payment system and a value loading system for a smart card using an open network such as the Internet.

BACKGROUND OF THE INVENTION
I 0 With the explosive growth in open networks (such as the Internet) over the past several years and the rapid increase in the number of consumers with access to the World Wide Web, there has been a great deal of interest in the development of electronic commerce on the Internet. Traditional financial transactions are being transformed.
A variety of service providers have introduced payment schemes to support the 1 5 purchase of goods or services on-line in a virtual merchant environment. These approaches have used several models based on traditional payment methods existing in the face-to-face retail market, including credit/debit cards, checks and cash. However, for a variety of reasons, various of these numerous schemes have particular drawbacks.

Currently, a consumer may use his or her traditional credit or debit card to make a purchase over the Internet. A consumer simply supplies his card account number which is then transmitted across the Internet to a merchant and the payment transaction is completed in the traditional manner for a credit card. Often, these account numbers are transmitted over the Internet with extremely limited or no security. Security can be improved through use of the "Secure Electronic Transaction" protocol published by Visa International and Mastercard in 1996. These transactions still require some form of card validation and performance of a balance check. These checks are performed on-line between the merchant, an acquirer and an issuing bank, a process which can become time consuming and inefficient when the value of the transaction is low, or when a number of small value transactions will be taking place in a short time span.
The electronic check is modeled on the paper check, but is initiated electronically using digital signature and public cryptography. Deposits are gathered by banks via electronic mail and cleared through existing channels such as the Automated Clearing House (ACH). However, use of such an electronic check by a consumer has various drawbacks. For one, digital signatures and public encryption necessitate use of a certifying authority adding additional entities and "net" trips to the transaction. Also, cardholder registration is needed.

Other Internet payment alternatives are modeled on cash transactions and include a variety of schemes. With CyberCash, the consumer appends his credit card number to an electronic invoice received from the merchant,

returns the credit card number to the merchant which is then processed and forwarded on to CyberCash where it is then treated like a normal credit card transaction. However, this technique suffers from some of the disadvantages discussed above with respect to traditional credit card transaction on the I 0 Internet and requires additional work by the merchant in processing the credit card number.

Debit transactions may also be completed but require a consumer to open a CyberCash account in advance.
A digital, token-based system for Internet transactions has been implemented by DigiCash. With DigiCash, so-called "digital coins" are purchased from DigiCash from a 1 5 prefunded deposit account and stored on the consumer's hard drive. These digital coins are then used for an Internet transaction with a merchant. This scheme has disadvantages in that the consumer must first set up a relationship with DigiCash and use a credit card or similar instrument to purchase these digital coins, which then must be downloaded to the consumer's computer. This transaction can be time consuming for the consumer and is subject to fraud. In addition, a merchant must be set up to not only accept these digital coins, but also to verify their authenticity, to confirm the transaction, and then finally to forward these numbers on to his bank in order to finally get paid. One drawback from the merchant's point of view is that much of the transaction work must be performed by the merchant.

Another scheme for completing an Internet transaction is offered by First Virtual Holding, Inc. First Virtual offers a software solution based upon a unique identification number and electronic mail confirmation, To use this scheme, a consumer opens a special account with First Virtual and then receives a confidential identification number. When the consumer wishes to purchase a product or service over the Internet, he or she sends an electronic mail message containing the confidential identification number to the merchant.

The merchant then sends the number to First Virtual by electronic mail

for verification and identification of the customer. First Virtual then confirms with the consumer by electronic mail that the consumer did indeed initiate the transaction and wishes to make the purchase.

There are drawbacks to this scheme in that the consumer must first open a special account with First Virtual. Also, the merchant must communicate with First Virtual to identify the customer and to identify the customer's credit card account number that is identified by the confidential identification number.

2
Aside from payment schemes over the Internet, a technique in use for performing a financial transaction at a stand-alone terminal uses a smart card. A smart card is typically a credit card-sized plastic card that includes a semiconductor chip for holding the digital equivalent of cash directly, instead of pointing to an account or providing credits. When a card of this kind is used to make a purchase, the digital equivalent of cash is transferred to the merchant's "cash register" and then to a financial institution. Stored-value cards are either replenishable (value can be reloaded onto the card using a terminal) or nonreplenishable (the card is decremented in value for each transaction and thrown away when all its value is gone).

to Physically, a smart card often resembles a traditional "credit" card having one or more semiconductor devices attached to a module embedded in

the card, providing contacts to the outside world. The card can interface with a point-of-sale terminal, an ATM, or a card reader integrated into a telephone, a computer, a vending machine, or any other appliance. A microcontroller semiconductor device embedded in "processor" smart card allows the card to undertake a range of computational operations, protected storage, encryption and decision making. Such a microcontroller typically includes a microprocessor, memory, and other functional hardware elements. Various types of cards are described in "The Advanced Card Report: Smart Card Primer", Kenneth R. Ayer and Joseph F. Schuler, The Schuler Consultancy, 1993, which is hereby incorporated by reference.

One example of a smart card implemented as a processor card is illustrated in FIG.

1. Of course, a smart card may be implemented in many ways, and need not necessarily include a microprocessor or other features. The smart card may be programmed with various types of functionality, such as a stored-value application; credit/debit; loyalty programs, etc. For the purpose of this disclosure, card 5 is programmed at least with a stored-value application, and will be referred to as "stored-value" card 5.

Stored-value card 5 has an embedded microcontroller 10 that includes a microprocessor 12, random access memory (RAM) 14, read-only memory (ROM) 16, non-volatile memory 18, an encryption module 22, and a card reader interface 24. Other features of the microcontroller may be present but are not shown, such as a clock, a random number generator, interrupt control, control logic, a charge pump, power connections, and interface contacts that allow the card to communicate with the outside Microprocessor 12 is any suitable central processing unit for executing commands and controlling the device. RAM 14 serves as storage for calculated results and as stack memory. ROM 16 stores the operating system, fixed data, standard routines, and look up
3
tables. Non-volatile memory 18 (such as EPROM or EEPROM) serves to store information that must not be lost when the card is disconnected from a power source but that must also be alterable to accommodate data specific to individual cards or any changes possible over the card lifetime. This information might include a card identification number, a personal identification number, authorization levels, cash balances, credit limits, etc. Encryption module 22 is an optional hardware module used for perfon-ning a variety of encryption algorithms. Card reader interface 24 includes the software and hardware necessary for communication with the outside world. A wide variety of interfaces are possible. By way of example, interface 24 may provide a contact interface, a close-coupled I 0 interface, a remote-coupled interface, or a variety of other interfaces. With a contact interface, signals from the microcontroller are routed to a number of metal contacts on the outside of the card which come in physical contact with similar contacts of a card reader device.

One possible use of a stored-value card by a consumer is illustrated in FIG. 2. FIG.

1 5 2 illustrates a block diagram of a customer operated service payment terminal 50. A customer typically uses such a service payment terminal in a face-to-face environment in order to purchase goods in a store or directly from the terminal itself. Service payment terminal 50 can be an attended device or it can be integrated into a self-service device such as a vending machine or public telephone. For example, the service payment terminal may be incorporated into a soda machine in order to

dispense sodas to a customer in which the customer pays by inserting the stored-value card. Or, the service payment terminal may be a point-of-sale terminal such as is found at a check-out counter where a customer inserts his stored-value card in order to purchase goods.

Service payment terminal 50 includes a router 5 1, a user interface 52, a card handler/reader 54, a security card handler 56, a security card 58, a terminal application 60, a data store 64 and a concentration point handler 66. Router 51 is hardware and software for routing information between functional blocks. User interface 52 controls the status of displays on the terminal and supplies instructions to the user. For example, the user interface provides instructions relating to insertion of stored-value card 5 or security card 58. Also, the user interface provides instructions and/or buttons for the customer to interact with terminal application 60 in order to purchase goods and/or services. Card handler 54 provides a physical card reader and associated software for accepting and communicating with stored-value card 5. Similarly, security card handler 56 provides a card reader and associated software for communicating with security card 58. In conjunction with security card handler 56, security card 58 controls the command sequence of the terminal and provides transaction and a batch security.
4
Terminal application 60 receives commands and information about the transaction and initiates the actual purchase. In addition, terminal application 60 is responsible for all application specific functionality such as guiding the customer through the use of the terminal via a display, and for providing all hardware and software needed to provide the user with a good and/or service once it has been informed by the security card that an appropriate value has been deducted from the stored-value card.

Data store 64 controls the storage of purchase transactions and totals.

Concentration point handler 66 controls the sending and receiving of information to and from a concentration point. Concentration point 68 is a staging computer that communicates with any number of service payment terminals to collect batches of transactions. The concentration point then sends these transaction batches to a clearing and administration system for processing (such as in FIG. 3). Once processed, batch acknowledgments, along with other system updates are sent to the terminals via the concentration point. The concentration point ensures a successful transfer of data between 1 5 service payment terminals and the clearing and administration system, and prevents overloading of the clearing and administration system. The service provider contracts with a concentration point for collection of the service payments. The concentration point may also be an existing central facility such as a telephone company that collects its own payments from card telephones.

Such a service payment terminal 50 allows a customer to use a stored-value card for the payment of goods and/or services, crenerates a payment result from a transaction, and bundles individual payment results into a collection for transfer to a clearing and administration system, which then transfers funds that had been debited from a customer's stored-value card to the merchant whose goods and/or services had been purchased from the terminal.

FIG. 3 illustrates an environment 100 useful for issuing stored-value cards and reconciling transactions perfon-ned with such a card. A ten-ninal supplier 102 builds the equipment used by a service provider 104 to provide goods and/or services to customers having a stored-value

card at a service payment terminal 50. Card Supplier 106 contracts with an integrated circuit manufacturer and a card manufacturer for integrated circuits and plastic card bodies, then embeds the integrated circuits into the cards and initializes them with a serial number. It then delivers the cards to card issuer 108. In conjunction with clearing and administration system I 10 (such as a system provided by Visa International of Foster City, CA), card issuer 108 personalizes new cards and then transfers these cards to individuals (cardholders 1 12). The cardholder may then charge the card with value prior to use. Alternatively, the card may come with value already loaded. The cardholder II 2 may then use the card at a service payment terminal 50 to purchase goods and/or services from
5
service provider 104. Terminal 50 then debits the value from the card, thus creating a service payment.

Periodically, all transactions are sent in a data file from terminal 50 via concentration point 68 and an acquirer 1 14 to clearing and batch administration system I IO along with accumulated service payment batches from other terminals. Based upon this collection data, clearing and administration system I 10 then receives money from card issuer 108 which had originally come from cardholder 1 12. Clearing and administration system I IO then transfers a lump sum to acquirer 1 14 using a suitable settlement service (such as one provided by Visa International) to pay the various service providers having a relationship with acquirer 1 14. Based upon the previous collection data, acquirer 1 14 then transfers an appropriate amount of money to each service provider 104 reflecting the value of the goods and/or services that that service provider had provided that day to cardholders based upon deductions from their stored-value cards.

Although such a service payment terminal described above is useful for the on-site 1 5 purchase of goods by a consumer with a smart card, it does not permit the purchase of goods and/or services by a customer over

a network. Nor does such a terminal permit the immediate transfer of electronic information to a consumer's computer. Service payment terminals are typically specially-designed units of hardware and software located at a merchant site. Furthermore, the service payment terminal is designed to integrate into one hardware location the functions of the terminal application (providing goods and/or services), a card handler for the stored-value card, and the transaction management embodied in the security card. Such a design is not suitable for transactions where a customer may wish to perforin a transaction from almost any location (including the home or office) quickly and easily with a minimum of prearranged set-up and expense.

Furthermore, although various Internet payment schemes have been suggested, they are not oriented toward small value transactions, and do not allow the use of a smart card for transactions over the Internet. Thus, it would be desirable to have an architecture and system that would allow a consumer to quickly and easily perform transactions over an open network such as the Internet using a smart card. It is also desirable to have an architecture and system in which a user may use a smart card for both purchases over the Internet as well as purchases at existing service payment terminals.

However, in order to purchase, the card must be loaded with value first. Value can be loaded onto a stored-value card in a variety of ways. Currently, it is inconvenient for a user to load value onto his or her

stored-value card. A user must physically travel to a bank or other institution that has an automated teller machine (ATM) or other similar device in
6
order to load value on to his or her stored-value card. The user can insert money into the machine and have a corresponding value put onto the stored-value card, the user can use a debit card to deduct value from the user's account at the bank for transfer to the card, or a credit card can be used as the source of funds to be transferred to the stored-value card.

In either case, the user must travel to the bank to load value. Further creating difficulty is that not all banks or other financial institutions have such a machine for loading value onto a user's stored-value card.

Accordingly, it would also be desirable to have a technique to allow a user to conveniently and easily load value onto a stored-value card.

I 0 SUMMARY OF THE INVENTION
To achieve the foregoing, and in accordance with the purposes of the present invention, an architecture and system is disclosed that enables the use of a smart card for payment of goods and/or services purchased on-line over an open network such as the Internet. Further, an architecture and system is disclosed that enables a smart card to be 1 5 loaded with value on-line over an open network such as the Internet.

In a first aspect, the present invention provides an electronic commerce payment solution offering consumers an on-line equivalent to purchases with cash or coins. It extends the notion of a smart card to the Internet marketplace, providing an alternative for low-value transactions. The present invention facilitates not only the purchase of physical croods, but also the purchase of digital merchandise (such as electronic information).
In one embodiment of the present invention, a client server on a client terminal controls the interaction with the consumer and interfaces to a card reader which accepts the consumer's smart card, which, in one specific embodiment, includes a stored-value application. For the purposes of this description, the smart card with a stored-value application used in embodiments of the invention will be simply referred to as a "storedvalue card." A payment server on the Internet includes a computer and terminals that contain security cards to handle the transaction, data store and collection. Also connected to the client terminal and the payment server over the Internet is a merchant server advertising the goods and/or services offered by a merchant for sale. In one embodiment of the invention, the merchant server includes a web site and the merchant has contracted with an acquirer to accept stored-value card payments for goods and/or services purchased over the Internet. Thus, a consumer may use his or her stored-value card at a client terminal location in order to purchase goods and/or services from a remote merchant server.

The Internet provides the routing functionality among the client tem-linal, merchant server and payment server.

7
From the consumer's perspective, the present invention operates in a similar fashion as using a stored-value card in a real merchant environment. The transaction process is similar to the interaction between a stored-value card and a service payment terminal in a face-to-face merchant environment, but with functionality distributed

across the Internet between the card reading device located where the customer is, the merchant server advertising the merchant's wares, and a payment server with a security card that manages the transaction. All of these entities may be physically remote from one another with router functionality being provided by the Internet. The present invention is easy to use. A consumer need not establish a new relationship with a bank or other Internet service I 0 company, nor create a special Internet deposit account in order to begin purchasing goods and/or services on the Internet. A consumer simply makes use of currently available stored-value cards in order to make an Internet purchase.

When browsing merchant store fronts on the Internet and deciding to purchase goods and/or services, the cardholder selects the stored-value card payment option offered by the 1 5 merchant. The cardholder then inserts his or her card into a card reader attached to a personal computer (for example). The cardholder's balance and purchase amount are displayed, the cardholder approves the purchase, and the amount is deducted from the value stored on the stored-value card. The transaction amount is captured by the security card or the merchant server for subsequent batch settlement through a clearing and administration system to the issuer and acquirer. In one embodiment, the transaction security and authentication for the system follows a similar methodology as that used in an actual service payment terminal between a stored-value card and the security card in the terminal. Advantageously, a customer may make use of pre-existing stored-value cards for purchases over the Internet without any prior arrangement of an account, purchases of credits or tokens, or establishment of a new relationship with a bank or other company.

In addition, once a value has been deducted from the stored-value card, the merchant has been informed, and the security card in the payment server has recorded the transaction, an existing clearing and administration system may be used to reconcile the transaction and to pay the appropriate parties. Advantageously, a new system and methodology for reconciling transactions need not be developed or implemented. A preexisting clearing and administration system may be used which greatly simplifies implementation of the present invention.

Use of a stored-value card as payment for Internet transactions provides numerous advantages. For example, a stored-value card can be used in small transactions where credit cards or checks would be unrealistic. Other advantages to the consumer include enhancing the value of a stored-value card by enabling access to both real and Internet merchant environments with a single card. The present invention also allows an
8
anonymous payment solution for transactions over open networks. Furthermore, in one embodiment of the invention the stored-value card is implemented on -a traditional credit card; a single card thus provides payment solutions for both low and high value transactions.

In addition, use of a stored-value card is extremely advantageous for small dollar amount transactions. Often, consumers are reluctant to use, and merchants are reluctant to accept, credit card transactions for small dollar amounts. For the consumer and the merchant dealing with many of these small transactions can be a bookkeeping headache and may not be worth the expense. A merchant may also be unlikely to accept a credit card for I 0 a small dollar amount transaction because of the service fees per transaction. By permitting the use of a stored-value card to make purchases over the Internet for small dollar amounts, a merchant may very well be able to begin charging for goods and/or services that he had

been providing for free in the past. One embodiment of the invention works well with purchases of under $ 1 0.00, although purchases of any amount may be made.

1 5 The present invention also provides numerous advantages to merchants who wish to sell goods and/or services over the Internet. For example, the present invention provides a payment solution for low-value transactions, enabling merchants to offer a wider range of digital merchandise. A merchant is also provided a method to recover costs of services not previously charged for, and is provided immediate access to an existing, and rapidly growing, cardholder base. Furthermore, the present invention integrates into an existing clearing and administration system meaning that the merchant need not implement or become familiar with new procedures for reconciliation of transactions.

Furthermore, a merchant need only make a minimal investment in time and money to take advantage of the present invention and to accept payments over the Internet. The merchant need not engage in the development of complex software or accounting procedures. Thus, smaller merchants will especially benefit from the present invention.

By establishing a business relationship with an acquirer and incorporating standard merchant software, a merchant is ready to begin selling goods and/or services from his web site. Because a smart card with a stored-value application is used, the payment server and the client terminal perform the details of the transaction and a merchant is

relieved from having to control and keep track of a transaction. Also, the payment server and its associated security cards manage and provide security for the transaction. From a merchant's point of view, the merchant knows that a consumer desires to purchase an item and that a cost has been transmitted to the consumer, thus, when the merchant receives a confirmation message, the merchant may release the item to the consumer. The merchant need not be concerned about security nor be responsible for authenticating a stored-value card nor for determining a balance on the card. Of course, a payment server could coexist
9
along with the merchant server or could even be the same computer. That is, a merchant could implement payment server functionality at its own site if it so desired.

In a second aspect of the present invention, a loading technique allows the consumer to conveniently load value on to his or her stored-value card from any suitable device via an open network such as the Internet. A consumer is allowed to use any suitable computer at the home, office or elsewhere in order to connect to his bank or other financial institution. Using appropriate message integrity, value is transferred from the bank to the consumer's stored-value card. At the same time, the corresponding value is transferred from the bank to the stored-value card issuer through existing networks for later settlement with a I 0 merchant from whom the consumer purchases goods or services. Advantageously, this embodiment makes use of an existing clearing and administration system for eventual settlement of the transaction between the merchant and the card issuer. Also, the transaction is fully auditable and a log of previous transactions is stored on the card for later display. Thus, a consumer may conveniently load value on to his or her card while a high 1 5 level of security is maintained and the card issuer can take advantage of unspent funds on the card.

From the consumer's perspective, the present invention operates in a

fashion similar to loading a stored-value card at an ATM machine, except that the consumer need not insert cash or an additional debit or credit card, nor need travel to a bank. The loading functionality is distributed across the Internet between the card reading device located where the customer is, a bank server holding the consumer's account, and a load server with a host security module that provides security. All of these entities may be physically remote from one another with router functionality being provided by the Internet.
Furthen-nore, a bank need only make a minimal investment in time and money to take advantage of the present invention in order to allow its customers to load value from their existing accounts over the Internet. The bank need not engage in the development of complex custom software or accounting procedures. By incorporating software libraries, a bank is ready to begin loading value onto its customer's cards from its web site.

Preferably, libraries are provided that interface with an existing server at a bank to facilitate the building of an HTML page. Because a smart card with a stored-value application is used, the bank server, load server and client terminal perform the details of the transaction and the bank itself is relieved from having to control and keep track of a transaction. Also, the load server and stored-value card manage and provide security for the transaction. Le., the bank need not be concerned about security nor be responsible for authenticating a stored-value card nor for determining a balance on the card. Of course, a load server could coexist alongside the bank server or could even be the same computer. That is, a bank could implement load server functionality at its own site if it so desired. In a preferred
10
embodiment, the load server and its security module is provided by a separate financial institution or by a third-party processor.
Both of the payment and loading aspects of the present invention provide benefits to issuers and acquirers. Expansion of the functionality for a stored-value card increases revenue opportunities from cardholders and merchants. Also, there may be new merchant marketing opportunities for acquirers. The present invention also offers a micro-payment solution for electronic commerce without the need to introduce a separate product or brand or to establish new service provider relationships. In addition, in one specific embodiment of the invention, funds that are loaded onto a card are transferred from the loading bank to I 0 the card issuer so that the issuer may take advantage of the funds on the card until they are spent.

A further advantage of both aspects of the present invention is its ability to minimize transaction traffic on the Internet and to minimize the amount of time that a security card (or a security module) is tied up with one transaction. In the payment aspect, by emulating 1 5 security card commands issued to a stored-value card, a client terminal is able to receive and group responses for transmission to a payment server all at once, rather than one-byone over the Internet. The payment server is then able to emulate a stored-value card as it interacts with the security card in delivering the responses to the security card. The result is less message traffic over the Internet, saving time and interrupts.
Also, by delivering an expected stored-value card signature to the payment server, the security card is relieved from having to compare the signatures itself, and may release sooner and move on to a new transaction. The payment server may also deliver the expected stored-value card signature to the client terminal or merchant server for comparison, thus reducing to one round trip the message traffic between the payment server and the client terminal.

The present invention is suitable for use with any type of stored-value card that is able to store an amount and to decrement a value upon a command. In one embodiment of the invention, a stored-value card implemented as a processor card works well. Use of a processor card has advantages where information processing is done on the card rather than in the terminal or host computer. Processor cards allow encryption to be done by the card, allow generation of signatures, and can accommodate multiple passwords or personal identification (such as biometrics that uniquely identify the holder of the card). Processor cards also provide increased data security, an anti-fraud capability, flexibility in applications, a multi-purpose capability, and off-line validation. Because high telecommunication costs and/or low reliability of a network may make on-line authorization
I I
impractical, a stored-value card with the capability for performing off-line processing and authentication by itself is extremely valuable.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention, together with further advantages thereof, may best be understood by reference to the following description taken in conjunction with the accompanying drawings in which.

FIG. I is a block diagram of an example of a stored-value card useful in embodiments of the present invention.

FIG. 2 is a block diagram of a service payment terminal in which a stored-value card may be inserted to purchase merchandise.

FIG. 3 is a block diagram of an example of a clearing and administration system useful for reconciling financial transactions received from a service payment terminal.

FIG. 4 illustrates an architecture and system for payment over the Internet using a stored-value card.

FIG. 5 illustrates a payment embodiment of the present invention.
FIG. 6 illustrates another payment embodiment of the present invention in which the security card releases earlier.

FIG. 7 illustrates yet another payment embodiment of the present invention having fewer round trip messages between the client terminal and payment server.

FIG. 8 illustrates still another payment embodiment of the present invention in which the merchant server compares stored-value card signatures.

FIG. 9 illustrates an added encryption layer useful for embodiments of the present invention.

FIG. 10 is a flowchart describing a user's perspective of a stored-value card purchase transaction using the present invention.

FIGS. I I A-I ID are a flowchart describing the processing of a user purchase using an embodiment of the present invention.

FIG. 12 is a flowchart describing the alternative embodiment of FIG. 6.
12
FIG. 13 is a flowchart describing the alternative embodiment of FIG. 7.

FIG. 14 is a flowchart describing the alternative embodiment of FIG. 8.

FIGS. 15A and 15B are a flowchart describing the added security layer of FIG. 9.

FIG. 16 illustrates an architecture and system for authentication over an intemet using a stored-value card.

FIG. 17 illustrates a system for loading value onto a stored-value card according to one embodiment of the present invention.

FIGS. 18A- I 8D are a flowchart describing the loading of a consumer's stored-value card using an embodiment of the present invention.

I 0 FIG. 19 is a block diagram of a typical computer system suitable for use in embodiments of the present invention.

DETAILED DESCRIPTION OF THE INVENTION
GENERAL ARCHITECTURE
The present invention separates the functionality involved in a transaction using a 1 5 stored-value card in order to take advantage of the routing capabilities of the Internet. FIG.

4 illustrates symbolically an architecture 200 for an internet payment system involving a smart card, such as a smart card having a stored-value capability. An internet loading system is shown in FIG. 17 and may have similar functionality as described below.

Shown is an internet 202, a client terminal 204, a payment server 206 and a merchant server 208. Local cardholder functions including a consumer card interface, display and accept/cancel options are performed at client terminal 204. Payment functions including security card control, data store and use of a concentration point are performed by payment server 206. The presentation and eventual delivery of goods and/or services by a merchant are performed under control of merchant server 208. The internet 202 performs routing functions between each entity. It should be appreciated that internet 202 may take the form of the Internet currently in use, or may also be any other open network implemented using any combination of computer, telephone, microwave, satellite, and/or cable networks.
Basically, client terminal 204 controls the interaction with a user and interfaces to card reader 210 which accepts a smart card having a stored-value application. For simplicity, throughout the remainder of

this specification, card 5 will be referred to as a stored-value card (SVC) 5. Payment server 206 communicates directly with a terminal or through a concentrator 212 that handles any number of tenninals 214-216 each having a
1 3
security card 218 and 220 respectively. Payment server 206 also communicates with concentration point 68 for transmission of transaction data to a clearing and administration system. Database 223 stores all suitable information passing through payment server 206 for each transaction. Use of such a database allows any number of merchants (or merchant servers) to use payment server 206 for transactions. Payment server 206 controls payment functions such as handling the attached terminals, managing data base 223 and collection functions. Merchant server 208 is a site that has contracted with an acquirer to accept stored-value card transactions as payments for goods and/or services purchased over the Internet.

I 0 Stored-value card 5 may take a variety of forms and is useful in many situations where it is desirable to store monetary value on a card that a consumer may use. In general, a stored-value card is any card or similar device that is able to store a value that is decremented when the card is used. The card may be purchased complete with a storedvalue or value may be later added to the card by a user. Such cards may also have their 1 5 value replenished. Of course, a stored-value card need not be in the form of the traditional credit card, but could appear in any form and of any material that is able to store value and be manipulated by a user for a payment transaction. By way of example, other forms that a stored-value card may take are any electronic representations. Further, the functionality of stored-value card 5 may be implemented in software on client terminal 204, that is, card 5 may be a "virtual" card.

A stored-value card may also perform a variety of functions in addition to simply storing value. A card may be dedicated to the storing value or may contain memory and programs for other applications as well. By way of example, an "electronic wallet" refers to a processor card that can execute a variety of financial transactions and identification functions. Such a card may serve debit, credit, prepayment, and other functions. A storedvalue card typically includes information such as a bank identifier number, a sequence number, a purchase key, a load key, an update key, an expiration date, a transaction counter, a session key, etc., in addition to a running balance.
A stored-value card may also be termed a prepayment card, a cash card, or a decrement-in-value card. A stored-value card may also be implemented by using a variety of card technologies. By way of example, a stored-value card is typically implemented as a card containing one or more integrated circuits. One example of an integrated circuit card is a memory card that has a semiconductor device for storing information but lacks calculating capability. Another example of an integrated circuit card is a processor card that has not only memory but also a microcontroller to enable the card to make decision. A processor card may also be termed a microprocessor card or a "smart card".

1 4
A processor card may include an encryption module in order to provide a variety of security precautions. By way of example, security precautions may include simple PIN numbers, biometrics, simple algorithms, or sophisticated algorithms such as the Data Encryption Standard (DES) or Rivest, Shamir, Adelman (RSA) encryption. The card is thus able to use these precautions to verify users, card readers, etc., to validate security cards and/or to provide a unique signature. Preferably card 5 includes any number of keys known to the card issuer that are used during the course of a payment or load transaction to generate signatures for validation of the stored-value card, validation of the security card or module, and validation of the system itself.

I 0 Client terminal 204 is any suitable device for interacting with a stored-valued card 5 and for communicating over a network to a payment server or a merchant server. By way of example, client terminal 204 may be a mainframe computer, a work station, a personal computer, a kiosk, or any type of service payment terminal that a consumer might use to purchase goods and/or services. Furthermore, client terminal 204 may also be embodied in 1 5 any portable device such as a laptop computer, a cellular telephone, or any variety of a personal digital assistant (PDA) such as those made by Apple Computer, Inc. or by U.S.

Robotics. Card reader 210 is any suitable interface device that functions

to transfer information and commands between client terminal 204 and stored-value card 5. By way of example, card reader 21 0 may be a card reader manufactured by Fischer-Farr International of Naples, Florida, by Hewlett-Packard of Palo Alto, California, by Schlumberger, by Gem Plus, etc. Card reader 2 1 0 may take any variety of forms such as a stand alone unit, integrated with the client terminal, attached to the keyboard of the client terminal, or even built in to a floppy disk-sized unit capable of being read from a disk drive of the client terminal, etc. Client terminal 204 includes client code module 224 and card reader module 226.

Reader module 226 may be implemented using any suitable software and libraries for communicating with card reader 2 1 0 and its actual implementation will depend upon the type of card reader used. Client module 224 controls communication between the client terminal, the card reader, the payment server and the merchant server. Client module 224 may be implemented using any suitable code. In one embodiment of the invention, client module 224 is implemented using a combination of "C" code and a Java applet. The applet is also supplemented with parameters from an HTML page sent from the merchant server.

It is contemplated that Java code works well for implementing the modules on the client, payment and merchant servers because it is platform independent, and could even replace the "C" and "C++" code used.

Client module 224 is also responsible for controlling displays to the user and for the interaction between the card and the card reader. The module also builds the draw request
1 5
message after receiving all of the start-up information from the card and the amount of the purchase from the merchant server. The client module is able to communicate with all components on the Internet, either directly or indirectly.

Payment server 206 includes payment code module 228 and terminal interface 230.

As with client ten-ninal 204, payment server 206 may be implemented using any suitable computer. By way of example, a personal computer works well. There may be one payment server for each merchant server or a single payment server may service any number of merchant servers. Alternatively, there may be multiple payment servers for a single merchant. In addition, payment server 206 need not be remote from merchant server 208 but may be located at the same site and have a different Internet address, or the payment server and the merchant server may even be implemented on the same computer.

Payment server 206 is designed to facilitate the communication between the user's storedvalue card and a terminal's security card. If a part of a transaction fails to complete, the payment server may notify the participating system components.
1 5 Payment module 228 may be implemented using any suitable code. By way of example, payment module 228 is implemented using a combination of "C" code, "C++" code and Java code. Payment module 228 is, in one specific embodiment, a multi-threaded process that can service multiple concurrent client applet transactions on demand. The module is responsible for controlling all interactions with the terminals and their concentrator including the transaction collection function. For individual transactions, the payment module controls the message flows and logs interim results. When an applet connects with the payment server, it

creates a transaction thread to support the transaction through its life cycle. Each thread, in turn, assigns a terminal for communication. Having a one-to-one correspondence between transaction threads and terminals has been found to provide desirable results.

Terminal interface 230 is any suitable set of software and libraries for communicating with a terminal 214 either directly or, as shown, through terminal concentrator 212. The actual implementation of terminal interface 230 will depend upon the type of terminal used.

A terminal such as 214 may be any suitable terminal such as are known in the art. By way of example, an iq Delta 2010 terminal made by Schlumberger has been found to provide desirable results. Such a terminal may support a variety of commands originating from the terminal interface. These commands emulate the non-nal responses that an attached terminal Security card 218 may be any suitable security card such as are known in the art (often referred to as a Purchase Secure Application Module--PSAM). In other embodiments, the functionality of security card 218 can be replaced by a hardware security module, could be implemented in hardware within the payment server, or could even be implemented in software.

By way of example, security card 218 is a removable crédit card-sized processor card that is programmed to process and store data relating to financial transactions. Security card 218 contains a microchip embedded in the card that enables the security card to authenticate and to validate the user's stored-value card. If a user stored-value card is accepted by the security card, and the stored-value card contains sufficient value, the security card guarantees that the merchant providing the goods and/or services receives payment according to the amount deducted from the stored-value card for the goods and/or services rendered. In a preferred embodiment, the security card also contains DES purchase security keys and authenticates the stored-value card during a purchase transaction 5 and secures the payment and collection totals. A

security card also stores signature algorithms for stored-value cards in use. A security card may also contain a transaction identifier for the current transaction, a financial sum of all transactions remaining to be settled, a session key, and master keys for all stored-value cards in use. Further, the security card may contain generations of keys, blocked card indicators, date of last update, multiple card programs, different currency rates and additional security.

Concentration point 68 is a staging computer that communicates with terminals to collect batches of purchase transactions. The concentration point then sends these transaction batches to a clearing and administration system for processing. Once processed, batch acknowledgments, along with other system updates, are sent back to the terminals via the concentration point.

Merchant server 208 includes a merchant code module 232. Merchant server 208 may be implemented upon any suitable computer capable of communicating with and presenting information to users over an intemet. Merchant code module 232 may be implemented using any suitable code. By way of example, merchant module 232 may be implemented using a combination of Perl, HTML, and Java code. Merchant server 208 is typically a generic web server customized for the merchant's business. Merchant server 208 may include databases, CGI scripts and back-office programs that produce HTML pages for an Internet user.

A brief discussion of the flow of a transaction now follows. During a financial transaction, the client terminal and merchant server exchange information 234 via internet 202. Each transaction initiated by a user has a transaction identifier created at the merchant
17
server, and a merchant identifier unique to the payment server is also available from the merchant server. Client module 224 and the payment server also use this unique transaction identifier for tracking and logging information about the transaction. Merchant server 208 generates a unique identification of the transaction, completes other required parameters, encrypts as appropriate, and builds an HTML page and sends it to the client terminal. The client module interacts 235 with the stored-value card and builds a draw request message containing related card information, the purchase amount, and other information supplied by the merchant server.

The client terminal then communicates 236 with payment server 206, first by I 0 forwarding the draw request to the payment server. Payment server 206 verifies the transaction to determine if it is a valid transaction from a known merchant. The transaction is logged into the payment server's transaction database 223. Upon completion of a transaction, payment server 206 builds a result message containing the identification of the transaction and signs it. The message is then routed to merchant server 208 via client 1 5 terminal 204. Merchant server 208 then validates the result message. After determining that the transaction was successful, merchant server 208 creates an HTML page for the purchased information and sends it to client terminal 204. Alternatively, the merchant may also deliver purchased goods to the user at this point. It is also possible for the payment server and the merchant server to communicate information 238 directly between themselves. Preferably, as client terminal 204 has already established communication with the merchant server and the payment server, links 234 and 236 are used to exchange information between the payment server and the merchant server, rather than establishing a new link 238.

USER PERSPECTIVE OF A PAYMENT TRANSACTION

FIG. 10 is a flowchart describing an embodiment of the present invention from a user's perspective such as may occur with the embodiment of the invention shown in FIG.

4. In step 502, a user acquires and adds value to a stored-value card. Alternatively, a user may acquire a stored-value card that already contains value. This stored-value card may take the form of any of the above-described stored-value cards that are able to store value and to debit value from the card. In step 504 the user accesses the merchant server web site via communication link 234 over the Internet. This access of a web site may be performed in any suitable fashion such as by using any commercially available web browser. In step 506 the user inserts a stored-value card in card reader 2 1 0 at the user's terminal.

Alternatively, the user may insert the card before accessing the web site, or even after the selection of goods and/or services from the merchant web site. In step 508 the user browses the merchant web site and selects goods and/or services for purchase from the merchant using the web site interface that the merchant has provided. The user then selects
1 8
an appropriate button on the merchant web site to indicate what the user wishes to purchase. Next, in step 5 10 the user receives a total sale amount from the merchant server and is directed to actuate a button on the web site indicating that the user wishes to proceed with the purchase

using the stored-value card.

In step 512 the architecture and system of the present invention (such as is shown in FIG. 4, for example) processes the user order by way of the payment server, terminal and security card. In step 514, the user's stored-value card is debited by the total sale amount and the user receives a "debited" message at the user's terminal. This message is optional if the system is designed so as to not inform the user of this debit. In step 516 the user receives a confirmation message from the merchant server indicating that the transaction has been completed. The user may now download the purchased information and/or receive a receipt for goods and/or services to be rendered or delivered from the merchant at a later date. In step 518 the merchant, via a clearing and administration system, receives payment to its bank account for the goods and/or services rendered by way of information collected from the payment server. In one embodiment of the invention, an existing clearing and administration system is used, as well as an existing methodology for transferring information from a security card for later reconciliation. This use of an existing "back end" allows systems of the invention to be implemented quickly and cheaply. This approach also ensures that cards used in the system are compatible with other stored-value terminals.

DETAILED PAYMENT TRANSACTION FLOW

FIG. 5 illustrates a detailed embodiment of internet payment architecture 200 having client terminal 204, payment server 206 and merchant server 208. A stored-value card 5 is in communication with client terminal 204, and a security card 218 inside a terminal 214 is in communication with payment server 206. Not shown for simplicity in this figure are other elements of the system shown in FIG. 4. One embodiment of a technique by which a financial transaction may be completed over the Internet will now be described using the flowchart of FIGS. I IA through I ID with reference to FIG. 5.

It should be appreciated that a wide variety of terminology may be used to describe message flow throughout the architecture. For example, the terminology used herein to describe the sequential messages draw request, debit, success, and confirmation, may also be referred to by the respective terminology: draw request, debit IEP, debit response, and debit result (or message result).

Initially, a suitable web browser of client terminal 204 is used by the user to access a merchant server web site as indicated by 302. In step 602, the user selects goods and/or
1 9
services from the merchant site and indicates to the site that the user wishes to purchase these items using a stored-value card as indicated at 304. In step 604 the merchant server receives this request for a stored-value card transaction.

In step 606 the merchant server builds an HTML page that includes the following client applet parameters: the total cost of the transaction as determined by the merchant server; the type of currency being used; the port and IP address of the payment server; a unique transaction identifier used by both the payment server and the merchant server to track a transaction; and a unique merchant identifier assigned to the merchant by the acquirer and known to the payment server. Other information may also be included such as I 0 the currency's exponent, a status URL address of the merchant server used for communication from the client terminal, and a merchant server generated key and other security information to ensure the identity of the merchant server and the integrity of the message. Other process related information such as

software release level, encryption methodology and keys may also be conveyed. Once this page has been built, the page is sent 306 to the requesting client browser and triggers the loading of the client code module (in this example a Java applet) in the client terminal.

Some browsers may not allow an applet to invoke a dynamic link library (DLL) due to security reasons. In an embodiment of the present invention, the client applet along with any DLLs needed are preloaded on the client terminal. Then, the merchant server is allowed to invoke the client applet and DLLs dynamically to circumvent this security precaution.
In step 608 the client module of the client terminal interacts with stored-value card 5 to obtain card information 308 in order to build a draw request message for later transmission 3 1 0 to payment server 206. In one embodiment of the invention, the client applet loads a local DLL, makes an API call to that library, which in turn makes a call to another DLL that finally makes a call to the card reader. In this fashion communication with the card is achieved. Once responses from the card are received, the client module will also combine these responses into a byte stream suitable for transmission over a network to a payment server. Also at this point, the currency type and expiration date on the card are checked, and the total cost of the ordered merchandise is checked against the card balance to ensure that the value on the card is great enough to cover the transaction. If the checks are not successful, a message to that effect is delivered to the user and this transaction terminates.

The client module emulates a variety of security card commands to receive responses from these commands from the stored-value card. Because the stored-value card and the security card are now physically separated from one another, and communication takes
20
place over the Internet, it would not be advantageous to engage in numerous commands and responses over such an open network. In the

interest of speed and reliability, it is advantageous to have fewer messages exchanged.

To operate securely and reliably in this environment, in one embodiment of the present invention, client module 224 emulates a security card and gathers all the responses for transmission in one draw request message. The draw request message may include a variety of information including a draw request token, state information, the merchant identifier, the transaction identifier, security information, a purse provider identifier, an intersector electronic purse (IEP) identifier, an algorithm used by the card, an expiry date, I 0 the balance of the card, a currency code, a currency exponent, the authentication mode of the IEP, the transaction number of the IEP, a key version and the purchase amount. As all of this information is prepackaged into a single draw request message, the number of messages between the stored-value card and the security card over the Internet is greatly reduced.

In this embodiment, the draw request message is built by packaging the stored-value card's response to the "reset" and "initialize" commands and any public key certificates along with the total cost and the currency of the transaction received from the HTML page.
For public key cards, the card and issuer certificates are obtained from read commands and may also be included in the draw request. By packaging all of this infon-nation together into one draw request message, it is possible to cut down on the number of messages exchanged between the client server and the payment server, and reliability and speed is improved. In one embodiment of the invention, an intersector electronic

purse JEP) protocol is used to reset and initialize the card and to receive a response.

Next, in step 6 1 0 the client terminal accesses the payment server using the IP address received from the merchant server. In step 612 the client terminal sends the draw request
messagetothepaymentserverasindicatedat3lO.
Theclientterminalalsocreatesalogof this message being sent.

In step 614 the payment server processes the draw request in conjunction with an associated security card as will be explained in greater detail below with reference to FIG.

1 ID. Draw request 312 is shown being sent to terminal 214. In one embodiment of the invention, the payment server creates a transaction thread for each connected client module to service it through the life cycle of the transaction. After step 614, the payment server has received a debit command and a security card signature 314 from the security card in the terminal. This debit command may also be termed a "debit I]EP" command. The security card signature is a value that uniquely identifies and validates security card 218 to prove to stored-value card 5 that the incoming debit command is a valid command from a real
21
security card. This validation ensures that when the stored-value card is debited, that the financial totals in the security card are updated. Thus, the user of the stored-value card is guaranteed that a valid debit of the card has occurred. In a preferred embodiment of the invention, the security card signature is an encrypted value ensuring that no other entity can forge an identity of a security card.

In step 616 the payment server sends the debit command along with the security card signature to the client terminal as indicated at 316 for the stored-value card to debit itself. At this time, the payment server also logs this debit command into its database.

In step 618, upon receiving the debit command from the payment server, the client module replaces the amount in the debit command with the original amount (from the merchant server) to ensure that the amount has not been tampered with while traveling over the network. At this time, the client module also creates a log of the debit command.

Client module 224 then passes 318 the debit command and security card signature to stored-value card 5 which verifies the signature, debits itself by the purchase amount, and 1 5 also generates a success message (also termed a "debit response" message) and a storedvalue card signature. The stored-value card signature is a unique value identifying a valid stored-value card. In a preferred embodiment of the invention, this signature is in encrypted form to prevent tampering. If card 5 does not have enough value to satisfy the purchase amount, then the "debit response" message indicates as such.

In step 620, card 5 sends a success message 320 along with the card signature back to client module 224 in client terminal 204. This success message may also be termed a "debit response" message. At this point, the purchase amount has been deducted from the balance on stored-value card 5. Next, in step 622, client module 224 packages the success message along with the card signature and sends them back to payment server 206 as indicated at 322. Client module 224 also logs the result of this stored-value card debit.
In step 624 the payment server receives incoming message 322 and creates

a log and updates the transaction status in its database for future error recovery. The payment server then directs this received message to the security card in the terminal as indicated at 324. Next, in step 626 the security card processes this response from the client's terminal and verifies the received stored-value card signature.

As the security card contains the keys and algorithms necessary to compute storedvalue card signatures, the security card is able to validate that a received stored-value card signature is in fact a valid one by comparing this stored-value card signature with a generated expected value. A successful comparison indicates that a success message 324 received from the stored-value card is in fact a valid success message and that the stored
22
value card has been debited. An error result code or a comparison that is not successful potentially indicates that the stored-value card has not been debited by the proper amount.

This comparison of stored-value card signatures by the security card ensures that a storedvalue card is in fact debited before the merchant server is directed to release the purchased merchandise. This comparison of the stored-value card signature to an expected value is performed by the security card for the highest level of security. As will be described in the embodiments of FIG. 6, 7, and 8, this comparison of stored-value card signatures may also take place in the payment server, in the client terminal or in the merchant server with a variety of other advantages. Assuming that the transaction is so far valid, in step 628 the I 0 security card sends a "confin-nation" message back to the payment server as indicated at
326. This confirmation message may also be termed a "message result." In step 630 the terminal updates its data store with the stored-value card number, a transaction count, the total sale amount, the response from the security card, and transaction numbers from the stored-value card and from the security card. The payment 1 5 server also logs the response received from the terminal including the merchant identifier, etc., as indicated in step 632. Next, in step 634, the payment server creates a confirmation message including the transaction identifiers and sends this message to the client terminal in encrypted form as indicated at 328. This message 328 may also be termed a "message
result."
By sending this confirmation message in encrypted form, the confirmation message may be passed to the merchant server by way of the client terminal without fear of tampering. As the confirmation message is encrypted, it would be extremely difficult for the client terminal or another entity to forge a confirmation message and trick the merchant server into thinking that a transaction had taken place. In another embodiment of the invention, if the client terininal is a trusted agent, then the confirmation message need not be encrypted. In yet another embodiment, the payment server may sent two confirmation messages, one not encrypted for the client to process, and one encrypted for the merchant server. FIGS. 15A and 15B present an embodiment in which the payment server sends two messages to the client terminal.

At this point, the transaction thread of the payment server that was used for the current transaction may release the terminal, thus allowing the terminal to be used by other transactions. This transaction thread then exits at this time.

In step 636 the client terminal then passes this confirmation message 330 on to the merchant server at the URL address previously received from the

merchant server.

Message 330 may also be termed a "message result." The client may also post a message to the user informing that the debit has been completed. The client also logs confirmation
23
of the payment. In step 638 the merchant server registers this confirmation message and checks for success. The merchant server calls a validate routine within the merchant code module with the confirmation message in order to validate the response from the client.

The validate routine is able to take the transaction identifier along with the encrypted confirmation message to decrypt the confirmation message. If the decrypted confirmation message is acceptable, the merchant server then determines a successful transaction has occurred. Next, in step 640 the merchant server generates an HTML page with the purchased information and delivers this infori-nation to the client terminal. Alternatively, the merchant server may generate a purchase receipt to deliver to the client terminal I 0 indicating goods and/or services to be rendered. At this point, the client terminal may also log the merchant server's response. Completion of these steps indicates a successful financial transaction over the Internet using a stored-value card.

Returning now to a more detailed discussion of step 614, FIG. I ID describes one technique for processing a draw request message in conjunction with a security card. Once 5 this draw request message has been received by the payment server and passed along to the terminal, the

terminal parses the message back into individual responses and passes these responses sequentially to the security card as will be explained below. In an alternative embodiment, a dumb terminal is used and the draw request is parsed into its components and otherwise processed by the payment server, which then sends the responses to the security card itself.

In step 680 the payment code module of the payment server edits the draw request for syntactic correctness and logs the draw request message as being received. In step 682 the draw request is passed to the terminal interface module of the payment server. In one specific embodiment, the terminal interface then requests a tern-iinal from the payment server's terminal pool. The payment server has a pool of terminals connected to the terminal concentrator that is established at start-up. At start-up, the payment server receives a list of all valid terminal identifiers. The payment server uses these identifiers, and its knowledge of transactions in progress to determine an appropriate terminal to process the transaction. Once a terminal is determined, the terminal interface builds a terminal specific message based upon the draw request and the type of terminal.
In step 686 the terminal specific draw request 312 is sent to the chosen terminal via the concentrator over a local area network. The concentrator acts as a router between a transaction thread in the payment server and its corresponding terminal. The concentrator looks at a header on the draw request to determine to which ten-ninal the transaction should be routed. In one embodiment of the invention, concentrator 212 is removed and payment server 206 communicates directly with ten-ninal 214 (for example).

24
In step 688 the terminal parses the draw request message into its various

components and processes each component in turn to emulate a stored-value card interacting with the security card in a physical terminal. Prepackaging of a variety of information into the draw request message results in fewer exchanges over the Internet between the client terminal and the payment server. By now simulating an interaction, the security card behaves as if it were in a physical terminal along with the stored-value card.

A variety of responses from a stored-value card may be emulated. In this embodiment, the terminal sends each of the three packages "answer to reset", "initialize IEP", and "debit" down to the security card individually and waits for a return message before sending the I 0 next response. For a public key transaction, the certificates read by the client are also included as individual responses. In this fashion, even though all of the stored-value card information (the draw request) originating from the client terminal has been sent at once in prepackaged form over the Internet, the traditional interaction between the stored-value card and the security card in a physical terminal may be simulated at the terminal in a remote 1 5 location.

In step 690 the terminal reaches a "draw amount" state, indicating that the security card is able to generate a debit command. In step 692, the security card generates its security card signature and the debit command. The debit command may also be termed a "debit IEP" command. This signature and debit command 314 are sent to the terminal.

The debit command issued by the security card may contain a wide variety of information including the security card identifier, the transaction identifier, the amount to be debited, the currency and currency exponent for the amount, the security card signature, the date, time, and location. The terminal in turn, sends the signature, command, and the terminal identifier to the payment server as indicated in step 694. The information may be sent to the payment server as indicated at 314 via a concentrator. At this point, step 614 ends and control returns to step 616.

FIRST ALTERNATIVE PAYMENT EMBODIMENT

FIG. 6 illustrates an alternative embodiment 200a in which the security card is able to be released sooner than the security card of FIG. 5; this embodiment also requires fewer exchanges between the terminal and the payment server. A security card in a terminal is dedicated to a particular transaction from the moment when the ten-ninal interface selects that terminal until the security card finally issues a "confirmation" message and is released by a terminal interface. Thus, in some circumstances it is desirable to release the security card earlier. By releasing a security card earlier, the card is tied up for a shorter time per transaction and may move on to the next transaction sooner. Also, the less time that a terminal is dedicated to a particular transaction, and the fewer messages exchanged between
25
the two, the less likely chance there is of a communication error that might interrupt and halt the transaction.

Embodiment 200a includes a client terminal 204, a payment server 206, a merchant server 208, a stored-value card 5, and a terminal 214 having a security card 218.

Communication between the various entities may take place in a similar fashion as in FIG.

5 as indicated by communication links 234, 235, and 236. However, instead of two round trips of information between the ten-ninal and payment server, there is only one round trip in this embodiment.

FIG. 12 is a flowchart that describes a technique for implementing this embodiment I 0 with reference to FIG. 6. Step 702 indicates that communication between the various entities takes place in a similar fashion as in FIG. 5 up until the terminal reaches the "draw amount" state. At this point, draw request 312 has been received and processed by the security card. Next, in step 704 the security card generates not only the security card signature and the debit command, but also an expected stored-value card signature. This 1 5 expected stored-value card signature is a value expected by the security card from the stored-value card to validate the stored-value card's success message. This validation will ensure that the stored-valued card has in fact debited itself.

In step 706 the security card signature, the debit command and the expected storedvalue card signature are sent to the payment code module in the payment server as indicated at 314a. Also, the terminal updates its data store in a similar fashion as in step 630. Next, step 708 indicates that the transaction occurs as before with reference to step 616 The steps indicate that the stored-value card receives the debit command, debits itself, and returns the success message (also termed a "debit response" message) and its card signature to the payment server.

Next, in step 7 1 0 the payment server code module processes this response from the stored-value card by comparing 346 the received card signature with the expected storedvalue card signature received earlier from the security card. This comparison of the two signatures by the payment module of the payment server foregoes the need for another round trip between the payment server and the security card. Because the security card has already delivered the expected card signature to the payment server, the security card may be released as soon as message 314a is received.

Assuming that the comparison is successful, the payment module is then able to generate its own confirmation message instead of waiting for a "confin-nation" message from the security card. Next, step 712 indicates that the processing continues in a similar fashion as in steps 632 The confirmation message is passed on to the merchant server
26
by way of the client terminal and the merchant server may then deliver the purchased merchandise to the user.

SECOND ALTERNATIVE PAYMENT EMBODIMENT

In another embodiment 200b of the present invention as illustrated in FIG. 7, not only is the security card allowed to release earlier, but the number of messages exchanged between the client terminal and the payment server are reduced. Instead of comparing stored-value card signatures in the payment server, the expected stored-value card signature from the security card is transmitted to the client terminal where a trusted agent 356 performs the comparison of the expected stored-value card signature with the actual signature received from stored-value card 5. Thus, message exchange between the client ten-ninal and the payment server is reduced to one round trip. This is advantageous in that the time for a transaction is reduced, the security card is released earlier and fewer message exchanges means more reliability over the Internet.

Embodiment 200b includes a client terminal 204, a payment server 206, a merchant server 208, a stored-value card 5. and a terminal 214 having a

security card 218.
Communication between the various entities may take place in a similar fashion as in FIG.

5 as indicated by communication links 234 and 235.

FIG. 13 is a flowchart that describes a technique for implementing this embodiment with reference to FIG. 7. Step 722 indicates that communication between the various entities takes place in a similar fashion as in FIG. 5 up until the terminal reaches the "draw amount" state. At this point, draw request 312 has been received and processed by the security card. Next, in step 724 the security card generates not only the security card signature and the debit command, but also an expected stored-value card signature.

In step 726 the security card signature, the debit command and this expected storedvalue card signature are sent to the payment code module in the payment server as indicated in 314a. Also, the terminal updates its data store in a similar fashion as in step 630. Next, in step 728 the payment server code module sends the debit command, merchant signature and expected stored-valued card signature to the client terminal.

Next, step 730 indicates that the transaction occurs as before with reference to steps 618 and 620. The steps indicate that the stored-value

card receives the debit command and debits itself. In step 732, the client code module itself compares the actual card signature from the stored-value card with the expected signature from the security card. This comparison of the two signatures by the client module of the client terminal foregoes the need for another round trip between the payment server and the client terminal. Also,
27
because the security card has already delivered the expected card signature to the payment server, the security card may be released as soon as message 314a is received.

Assuming that the comparison is successful, the client terminal is then able to generate its own confirmation message in step 734 instead of waiting for a confirmation message from the payment server. Next, step 736 indicates that the processing continues in a similar fashion as in steps 636 The confirmation message is passed on to the merchant server and the merchant server may then deliver the purchased merchandise to the user.

THIRD ALTERNATIVE PAYMENT EMBODIMENT
I 0 FIG. 8 illustrates another embodiment 200c of the invention in which the merchant server performs the comparison of the stored-value card signature with the expected signature. This embodiment has all of the advantages of the previous embodiment in which the security card is released earlier, and there are also fewer messages passed between the entities. In this embodiment, if the client terminal is not to be trusted to compare the stored1 5 value card signatures, then an encrypted signature is passed to the merchant server via the client ten-ninal. The client terminal also passes the raw, unencrypted signature from the stored-value card to the merchant server. A routine 366 in the merchant server then compares the two signatures.

Embodiment 200c includes a client terminal 204, a payment server 206, a merchant server 208, a stored-value card 5, and a terminal 214 having a security card 21 S.

Communication between the various entities may take place in a similar fashion as in FIG.

5 as indicated by messages 302-306 and communication link 235.

FIG. 14 is a flowchart that describes a technique for implementing this embodiment with reference to FIG. 8. Step 742 indicates that communication between the various entities takes place in a similar fashion as in FIG. 5 up until the ten-ninal reaches the "draw amount" state. At this point, draw request 312 has been received and processed by the security card. Next, in step 744 the security card generates not only the security card signature and the debit command, but also an expected stored-value card signature.

In step 746 the security card signature, the debit command and this expected storedvalue card signature are sent to the payment code module in the payment server as indicated in 314a. Also, the terminal updates its data store in a similar fashion as in step 630. Next, in step 748 the payment server code module sends the debit command, merchant signature and an encrypted expected stored-valued card signature to the client terminal. The expected stored-valued card signature is encrypted to prevent tampering by the client terminal or other outside entity.

28
Next, step 750 indicates that the transaction occurs as before with reference to steps 618 and 620. The steps indicate that the stored-value card receives the debit command and debits itself. In step 752, the client code module sends the success message, the raw stored-value card signature and the encrypted signature on to the merchant server. In step 754 the merchant server processes the success message, decrypts the encrypted signature, and compares the two signatures. This comparison of the two signatures by the merchant server foregoes the need for another round trip between the payment server and the client terminal. Also, because the security card has already delivered the expected card signature to the payment server, the security card may be released as soon as message 314a is received.

Assuming that the comparison is successful, the merchant server is then able to generate its own confirmation message in step 756 instead of waiting for a confirmation message from the client terminal. Next, step 758 indicates that the processing continues in a similar fashion as in steps 638 and 640. The merchant server may then deliver the 1 5 purchased merchandise to the user. In all of the above alternative embodiments, when the transaction is not completed successfully, the payment server reverses the transaction within the ten-ninal.

ENCRYPTION LAYER EMBODIMENT
FIG. 9 illustrates an embodiment 200d of the present invention in which an encryption layer has been added. Although the present invention may be practiced without this added encryption layer, in a preferred embodiment of the invention, this encryption layer is used. FIG. 9 includes client terminal 204, payment server 206 and merchant server 208. Other elements of the architecture have been omitted in this figure for simplicity.

This extra encryption layer is used not only to protect the contents of messages being transmitted over the Internet, but also to prevent a client terminal, stored-value card or other entity from receiving or producing a message that would trick another entity into thinking that a valid transaction had occurred. This encryption also prevents messages

from being accidentally or deliberately altered or misdirected.

It should be appreciated that encryption may be present in any embodiment on all parts of any message sent for security. Preferably, any signature sent over a network is encrypted.

Figures 15A and 15B are a flowchart describing this embodiment of the invention with reference to FIG. 9. In step 802, the payment server and the merchant server share a unique encryption key. Through a prior business arrangement, both of the servers have arranged to share this unique key to add security to the transaction. The shared key may be
29
of any suitable encryption standard and of any length. The key may be a Data Encryption Standard (DES) key having a length of 128 bits including parity. Although this shared key could be used directly, in a preferred embodiment of the invention, there is a derived unique key for each transaction between the merchant server and the payment server.

Alternatively, another encryption standard such as RSA may also be used. Preferably, loading of value is performed under DES, while a purchase may be performed under either DES or public key technology.

In step 804 the client terminal and the merchant server engage in a protected Secure Sockets Layer (SSL) session 404 in which a connection is made, a user browses and makes a purchase selection. The SSL session protects the information transmitted over the Internet such as card information, commands, and encryption keys from being discovered by an unauthorized party. Other techniques for protecting a session may also be used.

In step 806 the merchant server derives a key from the DES key using information unique to the transaction such as the merchant identifier, the transaction identifier, or other 1 5 information unique to this transaction, such as a random number. Because the payment server shares the DES key with the merchant server and also has access to this unique information about the transaction, the payment server will also be able to derive this same key from the shared DES key. In this step the merchant server also creates a transaction session key (TSK) for use by the client terminal and payment server in encrypting information.

In step 808 the merchant server downloads an HTML page of information 406 that includes the TSK and the TSK that is encrypted using the derived key (ETSK). The TSK encrypted with the derived key will be used by the payment server to return an encrypted (and unreadable by the client) confirmation message to the merchant server. Only the merchant server will be able to decrypt this confin-nation message and will thus be guaranteed that a successful transaction has occurred and that merchandise may be released to the client.

In step 8 1 0, the client prepares the draw request in conjunction with the storedvalue card and sends the draw request 408 encrypted with the TSK to the payment server along with the ETSK. In step 812 the payment server uses the shared DES key and the prearranged information unique to the transaction to derive the same key that the merchant server has used. Thus, the derived key can be used to decrypt the ETSK in order to produce the TSK. Once the payment server had produced the TSK, it may decrypt the draw request and process the draw request in any suitable fashion with the security card.
Once the payment server has received the debit command from the security card, it encrypts

the debit command with the TSK. The debit command may also be termed the "debit EEP
command."
In step 814 the payment server sends the encrypted debit command 410 to the client terminal. In step 816 the client decrypts the debit command with the TSK it had received earlier from the merchant server and processes the debit command in a suitable fashion with a stored-value card. Once the client terminal has received the debit response message from the stored-value card, it encrypts this message with the TSK and sends the debit response message 412 to the payment server. In step 820, the payment server decrypts the debit response message with the TSK and processes the debit response message in a suitable I 0 fashion with the security card.

Once the payment server has received a "debit result" message from the security card, the payment server encrypts the "debit result" message with the TSK to form a "debit result U message for the client. The "debit result C" message will be used by the client terminal to inform the user of a successful transaction. The payment server also generates its own 1 5 confin-nation message and encrypts the confirmation message with the derived key to form a "debit result M" message. The payment server then sends 414 the "debit result C" message and the "debit result M" message

to the client terminal.

In step 822 the client terminal decrypts and processes the "debit result C" message and passes the "debit result M" message 416 on to the merchant server. Because the "debit result M" message is encrypted with the derived key, the client terminal or other entity is not able to tamper with it. In step 824 the merchant server is able to decrypt the "debit result M" message because it had originally produced the derived key from the DES key.

Once the merchant server has determined that a valid "debit result M" message has been received, it confirms that a valid transaction has taken place and may release merchandise to the user.

This security embodiment of FIG. 9 may be used with any of the previously described embodiments of the invention. By way of example, this security embodiment may be used with the embodiments of Figures 7 and 8 in which there is only one round trip between the client terminal and the payment server. In particular, the expected stored-value card signature received from the security card may be encrypted with the derived key so that it unreadable by the client, yet the merchant server will be able to compare the received stored-value card signature with the expected card signature to validate the transaction.

A wide variety of terminology may be used to describe the keys described above.

For example, the keys referred to above as shared DES key, transaction session key (TSK) and derived key, may also be referred to as shared key, session C key and session M key.

3 1
AUTHENTICATION EMBODE
4ENT
FIG. 16 illustrates an architecture and system 200' for authentication over an internet (such as the Internet) using a pseudo stored-value

application. This application could reside on a stored-value card along with standard accounts, stored value, or other card applications. The card defines access to the pseudo stored-value service and ensures that the card is present and passes security checks.
In one embodiment of the present invention, a consumer may wish to access any of a variety of Web servers in order to redeem **frequent flyer miles** , award points, etc., that he or she has **accumulated** . In this embodiment, a consumer has accumulated "points" through any of a variety of programs with airlines, restaurants, rental car companies, hotels, banks, **credit** or debit card issuers, telephone or other communication **company** , etc.

The consumer wishes to redeem these points to receive free airline tickets, meals, car rental, overnight stays, prizes, awards, discounts, or other "benefits". By accessing a Web server associated with the particular program, the consumer is able to use his or her card in 1 5 any of the embodiments described herein to authenticate the card and to receive these benefits from the program. Most often, a card has a card number that is associated with the consumer's name in a database on the Web server. This card number is transmitted to the Web server as part of the card signature, or in a similar fashion. Thus, an authenticated card used in this embodiment to redeem services may be matched to the appropriate consumer.

For example, a consumer with 30,000 frequent flyer miles on one airline may use this embodiment of the present invention to access a Web server associated with the airline.

The consumer is requesting a free round-trip ticket in exchange for 20,000 miles. The present invention then operates to authenticate the consumer's stored-value loyalty application on the card, and delivers a confirmation of authentication message to the Web server for the airline. The Web server then deducts 20,000 miles from the consumer's account (leaving 10,000 miles) and delivers the free ticket to the consumer. In one specific embodiment, the Web server associated with the airline (or the airline itself) keeps track of the consumer's account and deducts the mileage. In this instance, an authentication application is used to validate the presence of the card or to obtain access to the Web server site.

In another specific embodiment, the consumer's card contains a loyalty application that stores the consumer's accumulated frequent flyer mileage; the mileage from the card is then debited and confirmed to the Web server in a similar fashion as described in various of the embodiments by which a cash value is stored on and debited from a card.

32
System 200' may be implemented in a similar fashion as system 200 of FIG. 4. The elements shown in system 200' having counterparts in system 200 are described above and have similar functionality. System 200' includes a web server 208' that may be any suitable computer server capable of presenting award information (hereinafter "benefits") to a consumer over an open network such as the Internet. Web server 208' may be the same as merchant server 208 of FIG. 4 or a separate computer. Preferably, web server 208' is implemented in a similar fashion as described above for merchant server 208. Web server 208' includes server module 232' that is preferably implemented in a similar fashion as merchant module 232. Additionally, server module 232' includes functionality to store and I 0 present benefits that are available for particular consumers. For example, benefits available such as airline tickets, prizes, etc., may be

presented.

Points (such as frequent flyer miles, for example) that a consumer accumulates to achieve benefits may be linked to a particular consumer by an account number, password, or other identifier. The amount of points accumulated for each consumer may be stored on 1 5 web server 208' using server module 232', or may be located in another database of the organization providing the benefits. In an alternative embodiment, these points for each program that a consumer is enrolled in are stored in a loyalty application on the consumer's card. For example, a consumer may have a stored-value card that in addition to storing monetary value, also stores a quantity of frequent flyer miles accumulated for a particular airline (or a number of airlines), points accumulated for using a particular credit card, points for hotel stays at particular hotels, etc. For points stored on the consumer's loyalty application card, these points may be verified and debited in much the same way that monetary value on the consumer's card is debited as described herein.

One embodiment by which a consumer has his or her pseudo stored-value application on a card authenticated to redeem points for benefits will now be explained. In one ific embodiment, a technique similar to that described in the flowchart of FIGS. I I A
speci
1 ID for debiting monetary value may be used. Initially, a user (consumer) operating client terminal 204 accesses web server 208' over link 234', views benefits presented for a particular program (such as an airline's frequent flyer program), selects benefits from that program, and requests the transaction to be performed using his or her pseudo stored-value application to validate that the card has access to the services. Web server 208' receives and processes this request. The above steps may be performed in a similar fashion as steps 602 and 604. Next, similar to step 606, web server 208' sends a page of information to client terminal 204. When claiming benefits, the total cost field is zero and the currency field is a specially assigned value. Keeping total cost field equal to zero causes the system to perform authentication but not to create a payment record. Alternatively, for those user's
33
whose card holds the amount of their points, additional fields may be sent from server 208' to terminal 204 indicating which account to debit and by how many points. The total cost and currency fields may be readily adapted for this purpose.

Next, in a similar fashion to steps 608 - 612, a draw request message is built, and the draw request is sent to authentication server 206' over link 236'. Similar to step 614, the authentication server now processes the draw request in conjunction with security card 218 (for example) and sends back a "debit" command and a security card signature to authentication server 206'. As total cost is zero, the "draw amount" state reached by security card 218 is also zero. In the alternative embodiment in which stored-value card 5 stores points for a particular program, total cost may be a value and a "draw amount" state may be reached indicating a number of points to be deducted from card 5. Next, similar to steps 616-618, authentication server 206' sends the debit command and security card signature to client terminal 204 and this information is processed by card 5. Even though a monetary value is not being debited, card 5 performs processing such as 1 5 incrementing a counter indicating number of transactions and generating a stored-value card signature. In the alternative embodiment in which points are stored on card 5, the points needed to redeem the benefit chosen by the user from web server 208' may be debited from the appropriate account in this

step.

Steps 620 through 638 are performed in a similar manner as in FIGS. I I B and I IC, except that in this case a monetary transaction is not being verified, but rather card 5 is being authenticated to allow the user to complete his access to services or benefits. In step 626 in particular, the signature of card 5 is verified by security card 218. In this embodiment, security card 218 would send an "authentication OK" message rather than the 4 4confirmation" message of step 628. Web server 208' then debits the appropriate number of points from the user's account or allows access to a privileged service for the benefit requested. In the alternative embodiment in which points are stored on card 5, the "authentication OK" message serves not only as an authentication of card 5, but also confirmation that the correct number of points have been debited from card 5 for the appropriate program. Next, similar to step 640, web server 208' releases the benefit requested by the user (such as airline tickets, prizes, discounts, etc.) and the benefit is arranged to be delivered to the user.

It should be appreciated that this technique of redeeming points for benefits may also be practiced using any of the alternative embodiments of FIGS. 6, 7 or 8, thereby obtaining the advantages associated with

those embodiments. Furthermore, this technique may take advantage of the encryption layer embodiment of FIG. 9. Additionally, as described
34
below, the present invention may also be used to load more points onto card 5 in much the same way that monetary value is added.

LOADING A STORED-VALUE CARD

FIG. 17 illustrates a system 850 for loading value onto a stored-value card according to one embodiment of the present invention. System 850 includes a client terminal 204, bank server 860 and load server 862. Client terminal 204 communicates with card 5 via card reader 2 1 0, and with bank server 860 and load server 862 over any suitable open network such as Internet 202. Suitable embodiments for the client terminal, the card reader and the stored-value card are described above in the description of a payment technique.

Preferably, each of client terminal 204, bank server 860 and load server 862 implement a code module (similar in operation to the code modules described above) in the Java programming language that provides the functionality described below. For simplicity of explanation, reference will be made below to "client terminal", "bank server" and "load server" even though the resident code is performing the functions. Card issuer 108 has been described previously in FIG. 3. Card issuer 108 may be a separate financial institution from the bank that includes bank server 860, or card issuer 108 may be the same bank that includes bank server 860.

Bank server 860 is any suitable computer within a bank or other financial institution.

By way of example, bank server 860 is any suitable personal computer, a workstation or a mainframe computer. In one embodiment, bank server 860 runs a "servIet" program (a Java applet running on server) for communication with client 204.

Load server 862 is also any suitable computer and may be located at a third party location (such as at a processor) or may be located within

the same bank as bank server 860. Load server 862 also runs a servIet program for communication with client terminal 204 and host security module 864. In an alternative embodiment, load server 862 and bank server 860 are the same computer which runs two different applications representing the functionality of each server.

Host security module (HSM) 864 is a device known in the art that may be embodied in a hardware "black box" or on any suitable computer. The host security module can be implemented in a hardware module outside of load server 862, can be implemented within load server 862, can be implemented in software, or can be implemented as a security card described above. Host security module 864 contains the encryption keys in hardware used for generating signatures (for example SI, S2 and S 3) that provide security for the transaction. These signatures are used by stored-value card 5 and host security module 864 to insure that the card is not expired or counterfeit (i.e., is a valid card), to insure that
35
module 864 is authentic, to insure that system 850 is authentic and, in general, to provide for a valid transaction and to prevent fraud. Card 5 also includes encryption keys for the generation of a stored-value card signature. In an alternative embodiment, module 864 could be replaced by a standard terminal that includes a security card such as is shown in the previous embodiments. In this situation, the encryption keys would be stored in the security card.

Briefly, system 850 operates as follows. A consumer accesses bank server 860 via client terminal 204. Assuming that card 5 is not overloaded and that the user's account with the bank has sufficient funds, the user is able to download value via bank server 860 on to his stored-value card 5. Client terminal 204 communicates with load server 862 to receive authorization for the load and for higher security. Card 5 may then be used to make purchases over the Internet as described earlier in the application or may be used for purchases elsewhere. Once the bank has downloaded value to card 5, a corresponding amount of funds is transferred from the bank to card issuer 108.

Card issuer 108 places these funds in a holding pool. Once stored-value card 5 is used to make a purchase from a merchant, the transaction is captured and settled through a settlement service, such as VisaNet. The issuer bank decrements the funds pool for the amount of the purchase, which is paid to the merchant bank. The merchant bank pays the merchant for the transaction. Settlement may occur in any suitable fashion such as is known in the art and, in particular, may be implemented as previously described in FIG. 3.

LOADING DETAILED TRANSACTION FLOW

One embodiment of a technique by which a stored-value card is loaded over the Internet will now be described using the flowchart of FIGS. 18A through 18D with reference to FIG. 17. Various of the steps below may occur in a different order; the following description is for illustration purposes. Interaction between client terminal 204 and bank server 860, and between client terminal 204 and load server 862, is preferably implemented in a similar fashion as between client terminal 204 and merchant server 208, and between client terminal 204 and payment server 206 as described above, respectively.

Certain implementation details mentioned above with respect to payment are equally applicable to loading a stored-value card. Furthermore, the exemplary flow shown in the figures illustrates a successful transaction (although a negative result is also explained below in the text). For

this reason, a "confirmation" message is referred to, which can more broadly be referred to as a "result" message (to reflect both the possibilities of success and failure of a load). Also, a "load success" message is referred to, which can also be referred to as a "confirmation" message, to reflect its status as either confirming a positive load result or a negative load result.

36
Initially, a suitable web browser of client terminal 204 is used by the user to access a bank server Internet site. In step 871 the user selects an option to load value onto card 5.

In step 872 the bank server sends a request for card information (including current card balance and maximum card balance); client terminal 204 reads the current card balance, currency, and other card information via card reader 2 1 0 and returns the balance to bank server 860. In step 873 the bank server determines the maximum load value and verifies that enough funds are in the user's account to accommodate a load request.

In step 874 the bank server builds an HTML page that includes the following client applet parameters: the load value; the type of currency being used; the port and IP address I 0 of the load server; a unique transaction identifier used by both the load server and the bank server to track a transaction; a unique bank identifier assigned to the bank and known to the load server; and a session key. Other information may also be included such as the currency's exponent, a status URL address of the bank server used for communication from the client terminal, and other security information to ensure the identity of the bank 5 server and the integrity of the message. Other process related information such as software release level, encryption methodology and keys may also be conveyed. Once this page has been built, the page is sent to the requesting client browser and triggers the activation of the client code module (in this example a Java applet) in the client terminal.

To determine the load value, the bank server requests that the user enter the amount to load to the card. Assuming that the user's account is adequate, the bank server requests the user's account be debited in step 875 by the load value. Advantageously, the debit request from the bank server can use the existing ATM and accounting systems of the bank to debit the user's account. From the bank's point of view, value is being transferred from the user's account much in the same way that value would be transferred to a user in the form of cash at an ATM. In this situation, though, the value is not being dispensed as cash at an ATM, but is being sent over the Internet to a stored-value card.

In step 876 the client terminal interacts with stored-value card 5 to obtain card information in order to build a load request message for later transmission to load server 862. Once responses from the card are received, the client terminal combines these responses into a byte stream suitable for transmission over a network to a load server.

The client terminal emulates a variety of host security module 864 commands to receive responses from these commands from the stored-value card. The stored-value card and the security module are physically separated from one another; communication takes place over the Internet. In the interest of speed and reliability, it is advantageous to have only the traditional authentication, response, and confirmation messages exchanged.

37
To operate securely and reliably in this environment, in one embodiment of the present invention the client ten-ninal emulates a security module and gathers all the responses for transmission into one load request message. The load request message may include a variety of information and preferably includes a first card signature (termed S 1), a card number, an expiry date, and a load amount. Other inforination such as the security algorithm, transaction counter, current card balance, and bank server time stamp are also preferably provided.

As all of this information is prepackaged into a single load request message, the number of messages exchanged between the stored-value card and the security module over the Internet is minimized.

Next, in step 877 the client terminal accesses the load server using the IP address received from the bank server. In step 878 the client terminal sends the load request message to the load server. In step 879 the load server processes the load request in conjunction with an associated host security module 864 as will be explained in greater detail below with reference to FIG. 18D. After step 879, the load server has received an issuer security module signature (termed S2) as part of a load command from the security module 864. The security module signature is a value

that uniquely identifies and validates the security module to prove to stored-value card 5 that the incoming load command is a valid command from a real security module. Thus, the user of the stored-value card, and other interested parties are guaranteed that a valid load of the card has occurred. In a preferred embodiment of the invention, the security module signature is an encrypted value ensuring that no other entity can forge an identity of a security module.

In step 880 the load server sends the load command including with the security module signature to the client terminal for the stored-value card to load itself. In step 88 1, upon receiving the load command from the load server, the client terminal passes the load command to stored-value card 5 which verifies the signature, loads itself by the load value, and also generates a load success message, a second stored-value card signature (termed S3), and a result code indicating success or failure of the load. In a preferred embodiment of the invention, this signature is in encrypted form to prevent tampering.

In step 882, card 5 sends load success message containing the card signature (S3) and result code back to client terminal 204. Next, in step 883 client terminal 204 packages the load success message along with the card signature and sends them back to load server 862. In step 884 the load server receives the incoming message. The load server then processes the message into its components and directs the components to the security module. Next, in step 885 the security module may process this response from the client's terminal and verify the received stored-value card signature (S3).

38
As the security module contains the keys and algorithms necessary to compute stored-value card signatures, the security module is able to validate that a received storedvalue card signature is in fact a valid one by comparing the received stored-value card signature with a generated expected value. A successful comparison indicates that a load success message received from the stored-value card is in fact a valid success message and that the stored-value card has been loaded. Assuming that the transaction is so far valid, in step 886 the security module

sends a "confirmation" message back to the load server.

It is possible that the stored-value card has not been loaded by the proper amount, that the card is invalid, a user is fraudulent or another discrepancy. For example, it is I 0 possible that a user has tampered with the card to make it appear that a load has not occurred, when in fact a load has occurred. In this situation, processing in step 882 and on is slightly different. For example, instead of generating a "load success" message, the card my generate a "negative result" code, potentially indicating that the card has not been loaded. Processing of this situation would then occur as follows.

1 5 In step 882, card 5 sends a load message containing the result code and stored-value card signature S3 back to client terminal 204. Client terminal 204 recognizes a negative result code, and invokes negative result handling. Client terminal 204 interacts with card 5 and generates a new load request for a zero value load using elements from the original request, along with a new card signature S 1.
The negative result code, along with the signatures S3 and new S 1, and the zero value load request are passed to the load server for analysis. The load server determines if the transaction counter in the zero value load equals the transaction counter in the previous request, along with verifying other pertinent information such as date and time, card number, and currency code and exponent. If the transaction counters are the same, then it is possible that a valid negative result has been received, but it should be verified because the client is not trusted. If the counters are equal, the load server will hold the original S3 and will generate a new load request to the security module using data element values that WO 98/49658 PCTIUS98/08806 On the other hand, if the transaction counters are not the same, then it is still possible that a valid negative result has been received, but it should be verified because the client is not trusted. First, the load server decreases the transaction counter in the new load request to match that of the original. The request along with the new S I is passed to the security module. The security module calculates its own new S I based upon the modified new load request. If there is no match, it means that the negative result was in error and that the card had been loaded. Processing continues to reflect a loaded card. If there is a match, it means the negative result was correct and that the transaction counter had been increased by accident. The user account is not debited, and not settlement occurs.
I 0 Returning now to further processing, in step 887 the load server logs the response received from the security module and updates its database with the transaction identifier, the bank identifier, the load value, etc. In general, any of the plethora of information passing through the load server may be added to its database. Next, in step 890 the load server creates a confirmation message including the transaction identifier and sends this 1 5 message to the client terminal in encrypted form. By sending this confirmation message in encrypted form, the confirmation message may be forwarded to the bank server by way of the client terminal without fear of tampering. As the confirmation message is encrypted, it In step 891 the client ten-ninal forwards the confirmation message on to the bank server at the URL address previously received from the bank server. The client terminal may also post a message to the user informing that the load has been completed. The client terminal also logs confirmation of the load. In step 892 the bank server registers the confirmation message. The bank server calls a routine to decrypt the confirmation message. If the decrypted confirmation message is acceptable, the bank server determines a successful load has occurred. The confirmation message provides assurance to the bank that the user's card was in fact loaded with a particular value and prevents fraud. For

example, a fraudulent user who tries to claim that his bank account was decremented and his card not loaded (and should thus receive more money from the bank) would be thwarted because the confirmation message proves that the user's card was in fact loaded.

Alternatively, the "confirmation" message may indicate that a load did not occur, in which case the account would not be debited, and no settlement would occur.

At this point a successful load of the user's card has occurred (assuming all is well).

For example, if the user had requested $ 1 00, that amount has been decremented from the user's account at the bank, and $100 has been loaded onto the user's stored-value card.

Preferably, at this point the amount loaded (in this example $ 1 00) is transferred from the bank to the stored-value card issuer preferably through an existing network. The $ 100 is
40
transferred so that the card issuer may manage the float on these unspent funds until the
userspendsthe$100. Oncethe$100(orasmallerportion)hasbeenspentwitha merchant, the card issuer is then able to settle the transaction with the merchant using any suitable clearing and administration system. In alternative embodiment, the bank may retain the $ 100 and settle directly with the merchant. In another embodiment, the bank and the card issuer are the same financial institution, and the $ 1 00 may be shifted between parts of the organization or remain in place.

Returning now to a more detailed discussion of step 879, FIG. I ID describes a technique for processing a load request message in conjunction with a security module.

I 0 Once the load request message is received by the load server, the load server parses it into the appropriate elements and passes a request to the security module as will be explained below. Alternatively, the load server can build a network message and switch the request to a remote authentication server. Or, a smart terminal could parse the message and pass responses to the security module.

5 In step 895 the load server edits the load request for syntactic correctness and logs the request as received. In step 896 the load server constructs a load request message. In step 897 the load server passes the load request to the security module to emulate a stored-value card interacting with the security module. The load server behaves as if a stored-value card were actually interacting in an ATM (for example) through a network to a host with a security module. In this fashion, the load request originating from the client terminal has been sent in prepackaged form over the Internet emulating a traditional interaction between the stored-value card in an ATM.

In step 898, the security module verifies the received stored-value card signature (SI) to prevent fraud. The security module generates its security module signature (termed S2) and the load command. The signature S2 will confirm to the client terminal and the storedvalue card that the host security module is authentic and belongs to the issuer of the storedvalue card. Additionally, S2 protects against a user trying to perforrn a fake load, keys out of synchronization, a counterfeit card, an expired card, etc. The security module then sends the signature and load

command to the load server as indicated in step 899. At this point, step 879 ends and control returns to step 880.

In another embodiment of the loading technique, a consumer may wish to access any of a variety of Web servers in order to load frequent flyer miles, award points, etc., that he or she has accumulated. A technique for authentication and redemption of such "points" is described above. In the loading embodiment, a consumer has accumulated points through any of a variety of programs with airlines, restaurants, rental car companies, hotels, banks, credit or debit card issuers, telephone or other communication companies, etc. These
4 1
points are stored by the particular airline, etc., that has issued them. The consumer wishes to load these points onto his or her stored-value card in order to redeem them elsewhere; thus receiving airline tickets, meals, car rental, overnight stays, prizes, awards, discounts, or other benefits. By accessing an Internet server associated with the particular

program.

the consumer is able to load his or her stored-value card in any of the embodiments described herein to receive the benefits of the program, much in the same way that currency is loaded.

COMPUTER SYSTEM EMBODIMENT

FIG. 19 illustrates a computer system 900 suitable for implementing an embodiment of the present invention. Computer system 900 includes any number of processors 902 (also referred to as central processing units, or CPUs) that are coupled to storage devices including primary storage 906 (such as random access memory, or RAM) and primary storage 904 (such as a read only memory, or ROM). As is well known in the art, primary storage 904 acts to transfer data and instructions uni-directionally to the CPU and primary 1 5 storage 906 is used typically to transfer data and instructions in a bi-directional manner.

Both of these primary storage devices may include any suitable of the computer-readable media described below. A mass storage device 908 is also coupled bi-directionally to CPU 902 and provides additional data storage capacity and may also include any of the computer-readable media described below. Mass storage device 908 may be used to store programs, data and the like and is typically a secondary storage medium (such as a hard disk) that is slower than primary storage. It will be appreciated that the information retained within mass storage device 908, may, in appropriate cases, be incorporated in standard fashion as part of primary storage 906 as virtual memory. A specific mass storage device such as a CD-ROM 914 passes data uni-directionally to the CPU.

CPU 902 is also coupled to an interface 9 1 0 that includes one or more input/output devices such as such as video monitors, track balls, mice, keyboards, microphones, touchsensitive displays, transducer card readers, magnetic or paper tape readers, tablets, styluses, voice or handwriting recognizers, biornetrics readers, or other computers. CPU 902 optionally may be coupled to another computer or telecommunications network using a network connection as shown generally at 912. With such a network connection, it is contemplated that the CPU might receive information from the network, or might output information to the network in the course of performing the above-described method steps.

Furthermore, method embodiments of the present invention may execute solely upon CPU 902 or may execute over a network connection such as the

Internet in conjunction with a remote CPU that shares a portion of the processing.

42
In addition, embodiments of the present invention further relate to computer storage products with a computer readable medium that have program code thereon for performing various computer-implemented operations. The media and program code may be those specially designed and constructed for the purposes of the present invention, or they may be of the kind well known and available to those having skill in the computer software arts.

Examples of computer-readable media include, but are not limited to: magnetic media such as hard disks, floppy disks, and magnetic tape; optical media such as CD-ROM disks; magneto-optical media such as floptical disks; and hardware devices that are specially configured to store and execute program code, such as application-specific integrated circuits (ASICs), programmable logic devices (PLDs) and ROM and RAM devices.

Examples of program code include machine code, such as produced by a compiler, and files containing higher level code that are executed by a computer using an interpreter.

Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be 5 practiced within the scope of the appended claims. For instance, any suitable stored-value card capable of loading, storing and decrementing value on command may be used with the present invention. Also, any network capable of performing routing functionality between a client terminal and a load and bank server may be used. Furthen-nore, the security module may be a physically separate module, a card located in a terminal attached to a load server, or its functionality may be incorporated directly into a load server in hardware or software. And although the client terminal may be used to route messages between the bank server and load server, both of these servers may also communicate directly between themselves, and may even be the same computer. The specific messages shown passing between the computers are exemplary, and other types of messages may be used. A specified load request is shown, but other information may also be loaded onto a storedvalue card using a security module emulation and then sent packaged as one message to the security module over a network. In addition to monetary value, other types of value such as electronic cash, checks, awards, loyalty points, benefits, etc., may be loaded onto a card, and the term '4value" is intended to broadly cover all these various types. Any suitable type of encryption may be used to encrypt messages passing between the computers. Therefore, the described embodiments should be taken as illustrative and not restrictive, and the invention should not be limited to the details given herein but should be defined by the following claims and their full scope of equivalents.

43

Claim
I A network payment system for transacting a sale of merchandise over a network
using a stored-value card, said network payment system comprising:
a router for routing communication between entities attached to said network; a merchant server in communication with said network, said merchant server

having at least a first item of merchandise for sale;
a client terminal in communication with said network, said client terminal including a card reader for communicating with said stored-value card, an output device for reviewing said first item for sale, and an input device for initiating a purchase transaction to
I 0 purchase said first item for sale; and
a payment server in communication with said network, said payment server including an inter-face for communicating with a security card and being arranged to receive a purchase message including an indication of said purchase transaction and to transmit a confirmation message to said merchant server over said network, whereby said merchant 1 5 server is authorized to release said item of merchandise to a user associated with said stored-value card. 2 . A network payment system as recited in claim I wherein said network is an internet and said merchant server includes a merchant web site for advertising said first item for sale over said intemet. 3 . A network payment system as recited in any of claims I or 2 wherein each of said client terminal, said merchant server and said payment server are at a separate location and communicate over said network. 4 . A network payment system as recited in any of claims 1-3 wherein said storedvalue card and said security card are both also suitable for use in an integrated service
payment terminal, and said network payment system further comprises:
a clearing and administration system for reconciling a plurality of transactions over said network. 5 . A network payment system as recited in any of claims 1-4 wherein said client terminal further includes a command emulator for emulating security card commands that are sent to said stored-value card and for grouping responses to said security card commands into a draw request message to be sent to said payment server, and said
44
payment server includes a response emulator for emulating responses from said storedvalue card that are sent to said security card. 6 . A network payment system as recited in any of claims 1-5 wherein said payment server includes a comparator for comparing a stored-valued card signature received from said stored-value card with an expected signature received from said security card to confirm a transaction, whereby the message traffic between said payment server and said security card is reduced. 7 . A network payment system as recited in any of claims 1-5 wherein said client terminal includes a comparator for comparing a stored-valued card signature received from said stored-value card with an expected signature from said security card received via said payment server to confirm a transaction, whereby message traffic between said payment server and said client terminal, and between said payment server and said security card is reduced. S. A network payment system as recited in any of claims 1-5 wherein said merchant server includes a comparator for comparing a stored-valued card signature received from said stored-value card with an expected signature from said security card received via said payment server, whereby a transaction is confirmed and whereby message traffic from said payment server, and between said payment server and said security card is reduced.

9 A computer-implemented method of selling merchandise over a network using a merchant server, said merchandise for purchase by a user with a stored-value card, said
method comprising:
establishing communication between said merchant server and a client over said
network;
receiving a request from said client to purchase an item available from said merchant

server;
transmitting to said client a purchase amount of said item so that said client may
debit a stored-value card associated with said client by said amount;
transmitting said amount, a transaction identifier and a merchant identifier to a payment server connected to said network, said transaction identifier uniquely identifying the purchase of said item and said merchant identifier uniquely identifying said merchant server to said payment server; and
a confirmation step for performing the function of confirming said purchase of said item to said merchant server, whereby said merchant server is informed that said sale of
45
said item is a success and said merchant server may release said item to said user associated with said stored-value card.

10 A method as recited in claim 9 wherein said network is an internet, wherein said merchant server includes a merchant web site for advertising said merchandise over said internet, wherein said client and said merchant server are at separate locations and said recited steps of said method occur over said internet.

11 A method as recited in any of claims 9 or 10 further comprising:
transmitting a key to said client for encrypting a draw request message

to be sent to
said payment server from said client terminal;
I 0 providing said key to decrypt said encrypted draw request message to said payment
server without sending said key in the clear to said payment server; and
receiving an encrypted transaction confirmation message from said payment server that is encrypted by a key shared between said merchant server and said payment server.

12 A method as recited in any of claims 9-1 1 wherein said step of transmitting said 5 purchase amount and said confirming step are routed through said client to provide communication between said merchant server and said payment server, whereby the number of communication links is reduced.

13 A computer-implemented method of transacting a sale of merchandise over a network using a client terminal in association with a stored-value card, said method
comprising:
transmitting over said network a request from said client terminal to purchase an
item available from said merchant server;
receiving from said merchant server an amount of a cost of said item;
sending a draw request message to a payment server connected to said network so that said draw request may be processed by a security card associated with said payment
server;
receiving a debit command from said payment server;
debiting said stored-value card associated with said client terminal by said amount;
and
46
sending confirmation information to said merchant server, whereby said merchant server is informed that said sale of said item is a success and said merchant server may release said item to a user associated with said

stored-value card.

14 A method as recited in claim 13 wherein said network is an internet, wherein said merchant server includes a merchant web site for advertising said merchandise over said internet, wherein said client terminal and said merchant server are at separate locations and said recited steps of said method occur over said internet.

15 A method as recited in any of claims 13 or 14 further comprising:
emulating security card commands that are sent to said stored-value card associated
I 0 with said client terminal; and
grouping responses to said security card commands into said draw request message so that said responses may be sent as a group to said payment server to reduce network traffic between said payment server and said client terminal.

16 A method as recited in any of claims 13-15 wherein said confirmation information 1 5 includes an encrypted confirmation message unreadable by said client terminal, said method
further comprising:
receiving said encrypted confirmation message from said payment server.

17 A method as recited in any of claims 13-15 wherein said confirmation information
includes a confin-nation message, said method further comprising:
receiving an expected stored-value card signature from said security card via said
payment server;
receiving an actual stored-value card signature from said stored-value card; comparing said actual stored-valued card signature received from said stored-value card with said expected stored-value card signature from said security card; and generating said confirmation message for transmission to said merchant server, whereby message traffic between said payment server and said client terminal, and between
In
said payment server and said security card is reduced.

18 A method as recited in any of claims 13-15 further comprising:
receiving an encrypted stored-value card signature from said security card via said
payment server that is unreadable by said client terminal;
47
receiving a raw stored-value card signature from said stored-value card; and transmitting to said merchant server as said confirmation infori-nation said encrypted stored-value card signature and said raw stored-value card signature for comparison by said merchant server, whereby message traffic between said payment server and said client tenninal, and between said payment server and said security card is reduced.

19 A method as recited in any of claims 13-18 further comprising:
receiving a security card signature for validating said security card to said storedvalue card, said security card signature being received in the same message from said
payment server as said debit command; and
I 0 receiving an expected stored-value card signature for comparison to an actual stored-value card signature, said expected stored-value card signature being received in the same message from said payment server as said debit command, whereby message traffic between said payment server

and said client terminal, and between said payment server and said security card is reduced. 1 5 20. A computer-implemented method of managing a transaction between a client terminal and a merchant server connected over a network, said transaction being managed by a payment server also connected to said network, said method comprising: receiving a draw request over said network, said draw request including an amount indicative of a cost of an item available from said merchant server, a transaction identifier uniquely identifying the purchase of said item, and a merchant identifier uniquely
identifying said merchant server to said payment server;
sending said draw request to a security card associated with said payment server so
that said draw request may be processed by said security card;
receiving a debit command from said security card;
sending said debit command from said payment server destined to said client terminal over said network so that a stored-value card associated with said client terminal
may be debited by said amount; and
a confirmation step for performing the function of confirming said purchase of said item to said merchant server, whereby said merchant server is informed that said purchase of said item is a success and said merchant server may release said item to a user associated with said stored-value card.
48
. A method as recited in claim 20 wherein said network is an internet, wherein said merchant server includes a merchant web site for advertising said item over said internet, wherein said client terminal and said merchant server are at separate locations and said recited steps of said method occur over said internet.

22 A method as recited in any of claims 20 or 21 wherein said stored-value card and said security card are both also suitable for use in an integrated service payment terminal,
'd method further comprising:
sal
sending transaction information regarding said sale of said item to a clearing and administration system for reconciling said sale.
I 0 23. A method as recited in any of claims 20-22 further comprising: receiving as part of said draw request responses from said stored-value card to security card commands that have been emulated by said client terminal; and emulating said stored-value card responses in an interaction with said security card to receive responses from said security card, whereby network traffic between said 1 5 payment server and said client terminal is reduced.

24 A method as recited in any of claims 20-23 wherein said confirmation step includes
the sub-steps of:
receiving a signature from said stored-value card associated with said client
ten-ninal;
sending said signature to said security card;
receiving a transaction OK message from said security card; and
sending a confirmation message destined for said merchant server.

25 A method as recited in any of claims 20-23 wherein said confirmation step includes
the sub-steps of:
receiving a signature from said stored-value card associated with said client

terminal;
comparing said received signature with an expected signature received from said
security card; and
49
sending a confirmation message destined for said merchant server, whereby message traffic between said security card and said payment server is reduced.

26 A method as recited in any of claims 20-23 wherein said confirmation step includes
the sub-steps of:
receiving an expected signature of said stored-value card from said security card;
and
sending said expected signature to said client terminal so that said client terminal may compare said expected signature to an actual signature of said stored-value card, whereby message traffic between said security card and said payment server, and between said client terminal and said payment server is reduced.

27 A method as recited in any of claims 20-23 wherein said confirmation step includes
the sub-steps of:
receiving an expected signature of said stored-value card from said security card; encrypting said expected signature so as to be unreadable by said client terminal;
and
sending said encrypted expected signature to said client terminal for resending to said merchant server so that said merchant server may compare said expected signature to an actual signature of said stored-value card, whereby message traffic between said security card and said payment server, and between said client terminal and said payment server is reduced.

28 A method as recited in any of claims 20-27 further comprising:
sending a security card signature for validating said security card, said security card signature being sent in the same message destined to said client terminal as said debit
command; and
sending an expected stored-value card signature for comparison to an actual storedvalue card signature, said expected stored-value card signature being sent in the same message destined to said client terminal as said debit command, whereby message traffic between said payment server and said client terminal, and between said payment server and said security card is reduced.
50
. A computer-implemented method of interacting with a stored-value card by a client terminal to facilitate the sale of an item of merchandise over a network, said method
comprising:
receiving a purchase amount for said item of merchandise from a merchant server
connected to said network;
emulating a plurality of security card commands that are sent to said stored-value
card associated with said client terminal;
receiving a plurality of responses to said security card commands from said stored
value card;

I 0 grouping said responses to said security card commands from said stored-value card together with said purchase amount to form a draw request message; and sending said draw request message to a payment

server over said network so that said draw request may be processed by a security card associated with said payment server to facilitate said sale of merchandise over said network, whereby network traffic between 5 said payment server and said client terminal is reduced.

30 A method as recited in claim 29 wherein said network is an intemet, wherein said merchant server includes a merchant web site for advertising said merchandise over said internet, wherein said client terminal and said merchant server are at separate locations and said recited steps of said method occur over said internet.

3 1. A method as recited in any of claims 29 or 30 further comprising:
receiving a debit command from said payment server destined for said stored-value
card, said debit command being generated by said security card;
receiving a security card signature for validating said security card to said storedvalue card, said security card signature being received in the same message from said
payment server as said debit command; and
receiving an expected stored-value card signature for comparison to an actual stored-value card signature, said expected stored-value card signature being received in the same message from said payment server as said debit command, whereby message traffic between said payment server and said client terminal, and between said payment server and said security card is reduced.

5 1
. A computer-implemented method of interacting with a security card to facilitate the
sale of merchandise over a network, said method comprising:
receiving a draw request message from a client terminal over said network, said draw request message including a plurality of responses from a stored-value card generated in response to emulation of security card commands, and also including a purchase amount for said merchandise, whereby network traffic between said payment server and said client terminal is reduced;
emulating said stored-value card responses in an interaction with said security card
associated with said payment server;
I 0 receiving a plurality of security card responses from said security card in response
to said emulation; and
sending a debit command destined to said client terminal over said network so that said debit command may be processed by said stored-value card associated with said client terminal to facilitate said sale of merchandise. 1 5 33. A method as recited in claim 32 wherein said network is an interriet to which is connected a merchant server having a merchant web site for advertising said merchandise over said intemet, wherein said client terminal and said merchant server are at separate locations and said recited steps of said method occur over said internet.

34 A method as recited in any of claims 32 or 33 further comprising:
a confirmation step for performing the function of confirming said sale of merchandise to said merchant server, whereby said merchant server is informed that said sale of said item is a success and said merchant server may release said merchandise to a user associated with said stored-value card.

35 A method as recited in any of claims 32-34 further comprising:
sending a security card signature for validating said security card, said

security card signature being sent in the same message destined to said client terminal as said debit
command; and
sending an expected stored-value card signature for comparison to an actual storedvalue card signature, said expected stored-value card signature being sent in the same message destined to said client ten-ninal as said debit command, whereby message traffic between said payment server and said client terminal, and between said payment server and said security card is reduced.
52
. A loading system for loading value over a network onto a stored-value card, said
loading system comprising:
a router for routing communication between entities attached to said network; a bank server in communication with said network, said bank server arranged to
debit a user account by an indicated value;
a client tenninal in communication with said network, said client terminal including a card reader for communicating with a stored-value card and an input device for indicating
a value to debited from said user account; and
a load server in communication with said network, said load server including an I 0 interface for communicating with a security module and being arranged to receive a load request including a stored-value card signature and being further arranged to transmit a confirmation message to said bank server over said network, thereby assuring that said stored-value card has been loaded by said indicated value.

37 A loading system as recited in claim 36 wherein said network is an internet and said 1 5 bank server includes a bank web site for accepting a load request.

38 A loading system as recited in any of claims 36 or 37 wherein said client terminal and said bank server are at separate locations and communicate over said intemet.
39 A loading system as recited in any of claims 36-38 further comprising:
a clearing and administration system for reconciling said debit of said user account with a purchase using said stored-value card.

40 A loading system as recited in any of claims 36-39 wherein said client terminal further includes a command emulator for emulating security module commands that are sent to said stored-value card and for grouping responses to said security module commands into a load request message to be sent to said load server, and wherein said load server includes a response emulator for emulating responses from said stored-value card that are sent to said security module.

41 A loading system as recited in any of claims 36-40 wherein said security module includes a comparator for comparing a stored-valued card signature received from said stored-value card with an expected signature to confirm a transaction.

42 A computer-implemented method of loading a stored-value card over a network
comprising:
53
establishing communication between a bank server and a client over a network; receiving a request from said client to load value onto a stored-value card; transmitting to said client a verified load value so that said client may load a stored

value card associated with said client by said load value;
transmitting to said client an address of a load server so that said client may send a
load request to said load server; and
a confirmation step for performing the function of confirming the loading of said stored-value card, whereby said bank server is assured that the loading is a success.

43 A method as recited in claim 42 wherein said network is an internet over which said recited steps of said method occur, wherein said bank server includes a bank web site for accepting a load request, and wherein said client and said bank server are at separate locations.

44 A method as recited in any of claims 42 or 43 wherein said confirmation step includes receiving a confirmation message that originates from one of said load server and a 1 5 security module associated with said load server.

45 A method as recited in any of claims 42-44 further comprising:
transmitting a first key to said client for encrypting a load request to be sent to said
load server;
providing said first key to decrypt said encrypted load request to said load server
without sending said first key in the clear to said load server; and
receiving an encrypted confin-nation message from said load server that is encrypted by a second key shared between said bank server and said load server.

46 A method as recited in any of claims 42-45 further comprising:
debiting a user account by said load value; and
sending transaction information including said load value to a stored-value card issuer for later settlement.

47 A computer-implemented method of loading a stored-value card over a network
comprising:
54
transmitting over a network from a client terminal to a bank server a request to load
a stored-value card;
receiving from said bank server a verified load value;
sending a load request to a load server connected to said network;
receiving a load command from said load server;
loading said stored-value card by said load value; and
sending confirmation information to said bank server, whereby said bank server is assured that said loading is a success.

48 A method as recited in claim 47 wherein said network is an internet over which said I 0 recited steps of said method occur, wherein said bank server includes a bank web site for accepting a load request, and wherein said client terminal and said bank server are at separate locations.

49 A method as recited in any of claims 47 or 48 further comprising:
emulating security module commands that are sent to said stored-value card
1 5 associated with said client terminal; and
grouping responses to said security module commands into said load request so that said responses may be sent as a group to said load server to reduce network traffic between said load server and said client

terminal.

50 A method as recited in any of claims 47-49 wherein said confirmation infori-nation includes an encrypted confirmation message unreadable by said client terminal, said method
further comprising:
receiving said encrypted confirmation message from said load server.

51 A computer-implemented method of managing a stored-value card load transaction between a client terminal and a bank server connected over a network, said method
comprising:
receiving by a load server over said network a load request, said load request
including a stored-value card signature;
55
sending said stored-value card signature to a security module associated with said load server so that said stored-value card signature may be validated by said security
module;
receiving a load command from said security module;
sending said load command from said load server destined to said client terminal so that a stored-value card associated with said client terminal may be loaded by a load value;
and
a confirmation step for performing the function of confirming the loading of said stored-value card, whereby a bank server is informed that the loading is a success. I 0 52. A method as recited in claim 51 wherein said network is an internet over which said recited steps of said method

occur, wherein said bank server includes a bank web site for accepting a load request, and wherein said client terminal and said bank server are at separate locations.

53 A method as recited in any of claims 51 or 52 further comprising:
receiving as part of said load request responses from said stored-value card to security module commands that have been emulated by said client terminal; and emulating said stored-value card responses in an interaction with said security module to receive responses from said security module, whereby network traffic between said load server and said client terminal is reduced.

54 A method as recited in any of claims 51-53 wherein said confirmation step includes
the sub-steps of:
comparing said received stored-value card signature with an expected signature; and sending a confirmation message destined for said bank server, whereby said bank server is assured that said stored-value card has been loaded.

55 A computer-implemented method of interacting with a stored-value card by a client terminal to facilitate the loading of said stored-value card over a network, said method
comprising:
receiving a load value from a bank server connected to said network;
emulating a plurality of security module commands that are sent to said stored-value
card associated with said client terminal;
56
receiving a plurality of responses to said security module commands from

said
stored-value card;
grouping said responses to said security module commands from said stored-value
card to form a load request; and
sending said load request to a load server over said network so that said load request may be processed by a security module associated with said load server to facilitate the loading of said stored-value card over said network, whereby network traffic between said load server and said client terminal is reduced.
56 A method as recited in claim 23 wherein said network is an internet over which said recited steps of said method occur, wherein said bank server includes a bank web site for accepting a load request, and wherein said client tenninal and said bank server are at separate locations.

57 A method as recited in any of claims 55 or 56 further comprising:
receiving an encrypted confirmation message from said load server that is unreadable by said client terminal; and
sending said encrypted confirmation message to said bank server, whereby said bank server is assured that said stored-value card has been loaded.

58 A computer-implemented method of interacting with a security module by a load server to facilitate the loading of a stored-value card over a network, said method
comprising:
receiving a load request from a client tenninal over a network, said load request including a plurality of responses from a stored-value card generated in response to emulation of security module commands, whereby network traffic between said load server
and said client ten-ninal is reduced;
emulating said stored-value card responses in an interaction with said security
module associated with said load server;
receiving a plurality of security module responses from said security module in
response to said emulation; and
sending a load command destined to said client terminal over said network to facilitate loading of said stored-value card.
57
. A method as recited in claim 58 wherein said network is an internet over which said recited steps of said method occur, and wherein said client ten-ninal and said load server are at separate locations.

60 A method as recited in any of claims 58 or 59 further comprising:
a confirmation step for performing the function of confirming loading of said stored-value card, whereby said bank server is assured that said stored-value card has been loaded.
58

Patent and Priority Information (Country, Number, Date):
Patent: ... **19981105**
Fulltext Availability:
Detailed Description
Publication Year: **1998**

Detailed Description
... may wish to access any of a variety of Web servers in order to redeem **frequen**t flyer miles , award points, etc., that he or she has **accumulated** . In this embodiment, a consumer has accumulated "points" through any of a variety of programs with airlines, restaurants, rental